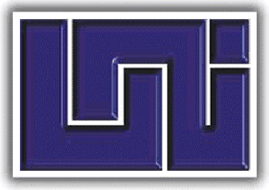


UNIVERSIDAD NACIONAL DE INGENIERIA

FACULTAD DE CIENCIAS Y SISTEMAS

MONOGRAFÍA PARA OPTAR AL TÍTULO DE
INGENIERO DE SISTEMAS

"PROPUESTA DE NORMATIVAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA PARA EL USO ADECUADO DE LOS ACTIVOS DE CÓMPUTO CONECTADOS A LA RED LAN DEL COMPLEJO NACIONAL DE SALUD "DRA. CONCEPCIÓN PALACIOS."

Elaborado Por:

Br. Zoila Rosa Porras Silva *95-11743-0*

Tutora: *Ing. Patricia Lacayo Cruz*

Asesores: *MSC. Germán López Quintana*
Ing. Carlos Rodríguez

Managua, 9 de julio del 2010.

ÍNDICE

DEDICATORIA

❖

❖ *A Dios todo poderoso, quien me ha dado la fuerza, valor y sabiduría para salir adelante. En su palabra dice: Mira que te mando que te esfuerces y seas valiente; no temas ni desmayes, porque Jehová tu Dios estará contigo en donde quieras que vayas. Josué 1:9*

❖

❖ *Mi padre Gonzalo Daniel Porras Silva, quien con su apoyo incondicional pude alcanzar mis objetivos.*

AGRADECIMIENTOS

- *Tutora Ing. Patricia Lacayo Cruz, cuyos conocimientos y experiencias me permitió culminar este trabajo.*

- *Asesores Msc. Germán López Quintana y al Ing. Carlos Rodríguez quienes fueron elementos esenciales para el desarrollo y culminación de este proyecto.*

- *Al personal informáticos del Ministerio de Salud, por sus recomendaciones y sugerencias para la culminación de este proyecto.*

- *A mi esposo Luis Manuel Espinoza Mendoza por su apoyo incondicional.*

RESUMEN

La técnica empleada en esta investigación es la realización de un diagnóstico del estudio técnico del sistema de tecnología de hardware y software y red del Ministerio de salud, se detallan en este estudio las especificaciones de topología informáticas y una breve descripción de la administración y nodo de la red. Además de un análisis funcional de la división de sistemas de información proponiendo fichas ocupacionales para ser agregada al manual de funciones para un mejor desempeño.

Así mismo se realizó una evaluación de riesgos para mitigar los problemas generados por las conexiones de internet; esto permitió aplicar un instrumento de medición cualitativo y cuantitativo para valorar el grado de inseguridades que inciden sobre los activos de comunicaciones para la generación de implementación de normativas de seguridad bajo los criterios de disponibilidad, confidencialidad e integridad de la información.

En base a la evaluación para mitigar los riesgos, se presentara a la institución las medidas de seguridad informática algunos manejos del software libre Nagios, herramienta para controlar los problemas informáticos generados por el tráfico de la red. Así mismo, la implementación del software libre OCS Inventory para un control de inventarios de los hardware y software instalado en los ordenadores de una red local, con un giro de negocio análogo al Ministerio de Salud, lo cual permitirá mejores práctica de seguridad en áreas sensible, y el documento tecnológicos de normativas basadas en la ISO/IEC 27001.

I. INTRODUCCIÓN

La división de sistema de información del Complejo Nacional de Salud "Dra. Concepción Palacios", no ha considerado al momento, ninguna práctica de uso de normativas de seguridad informática para la administración del equipamiento de cómputos incorporados en la Intranet.

Esta tecnología, enfrenta distintos tipos de riesgos e inseguridades, que pueden surgir de fuentes no fiables y/o maliciosas tales como fraudes informáticos, espionaje, virus, denegación de servicios y daños a los sistemas operativo; además, del alto costo que con lleva el mantenimiento correctivo y preventivo, debido a los malos manejos asociados al desconocimiento de prácticas adecuadas, regidas por normativas de seguridad informáticas.

El documento incorpora en sí, el uso de normativas de seguridad tecnológicas de la información como herramienta orientada a la protección de los activos informáticos conectado a la red LAN de este Complejo de Salud Pública.

La Organización Internacional de Estandarización (ISO/IEC17799) ha incorporado en sus normas una segunda versión, que es el estándar de gestión de seguridad de la información ISO/IEC 27001, donde se establece la metodología de buenas prácticas para la seguridad de las comunicaciones teniendo por objeto, ayudar a las organizaciones al establecimiento y mantenimiento en sus tecnologías.

Estas normativas brindan unas series de recomendaciones para la seguridad de los activos informáticos, proponiendo una base común en un sistema de comunicación eficaz, orientado a los procesos de los sistemas más importantes de la Institución, caso típico aplicado al MINSA.

En este estudio, se detectaron los riesgos que ocasionan los problemas de seguridad a los activos conectado a la red LAN. Se efectuó una evaluación de riegos informáticos para medir el grado de afectación y frecuencia de aparición, así mismo, la causa y el efecto que inciden sobre los activos de cómputos, asignándoles una calificación con valores predeterminados midiendo el daño sobre los equipos automatizados. Esta valoración se ejecutó en conjunto con el área de informática de la institución en mención.

Se presentará a la institución un documento tecnológico con lineamiento de seguridad para proteger los equipos y sistemas informáticos bajo la normativa ISO/IEC 27001 cuyas ventajas estarán determinadas por la aplicación de lineamientos de seguridad informática en área sensibles; la generación de una buena administración de los equipos de cómputos conectados a red; la protección de los equipos informáticos utilizando herramienta para una buena administración; minimizando los riesgos de falla en la operación y daño de la infraestructura tecnológica; el aumento de la motivación y satisfacción del personal; prolongando la vida útil de los equipos y componentes de la red; realizando una evaluación de riesgos informáticos con el fin agregar nuevas normativas de seguridad informática para uso adecuados de los activos y servicios conectados a red.

II. ANTECEDENTES

La utilización de la tecnología informática del Complejo Nacional de Salud"Dra. Concepción Palacios" inició a principios de la década de los 90, con muy pocas máquinas dedicadas, a la automatización de los procesos realizados. La cantidad de usuarios fue aumentando, así la cantidad equipos, esto obligo a la necesidad de conectarlos entre sí a una red con servicios de internet. En un principio, este proceso se realizó de forma ordenada; pero, con el paso del tiempo los equipos se conectaron de acuerdo a las necesidades inmediatas de la empresa y no hubo un plan previamente establecido para administrar los dispositivos conectados a red.

Es, hasta estos últimos años que se han empezado a realizar esfuerzos con miras a organizar la seguridad de la información es la parte fundamental de la organización funcional de la división de sistemas de información.

El manejo de la información sobre los proyecto de salubridad a nivel nacional, el presentar a otra instituciones del estado la distribución de entradas y salidas del presupuesto para la salud pública, han avanzado en los últimos años por que las actividades que se realizan son digitalizadas. Estas mejoras se han extendido tanto que se ha creado un estándar universal sobre el manejo de la información.

El principal problema ha sido que la red existente no ha sido construida de acuerdo a un plan estratégico a nivel de seguridad, ni está sujeta a un estándar de confianza. El área de informática no ha sido tratada con la importancia que merece, hasta hoy. El proyecto de creación, de más punto de red sobre la infraestructura informática de redes en el Ministerio de Salud, es el primero que se ha formulado con un objetivo claro y definido apoyados en las experiencias de los servicios de salud de otros países adelantados tecnológicamente.

III. DEFINICIÓN DEL PROBLEMA

La observación en el departamento de informática nos permitió constatar los problemas organizativos existentes tanto informáticos como laborales, que se ven reflejados en la carencia de una adecuada asignación de tareas a cada uno de los integrantes del área.

También se pone de manifiesto en el retraso de la realización del los mantenimiento correctivo y preventivos por parte de los informáticos de soporte técnicos. Esto se debe a que, no hay una coordinación de las funciones correspondientes a su cargo laboral.

La falta de planificación dificulta el establecer una relación de las oportunidades de los sistemas de información y las nuevas tecnologías; el aprovechamiento de las futuras inversiones en la certificación de los sistemas de información; el evitar inconsistencias e incompatibilidades de la información; el mantener una estandarización en interfaces.

El Ministerio de Salud, carece actualmente de la autonomía financiera suficiente para integrar un sistema de Gestión de Seguridad de la Información basados en el código de buenas prácticas de confianza computaciones, que le permita responder mejor a las necesidades de los clientes y ser más competitiva a nivel internacional. Por lo tanto, la presente investigación es requerida como una colaboración de la universidad a una empresa del estado.

La carencia de información clara para formular un plan de seguridad, que permita definir las normativas de confianza a los recursos que se deben proteger y la falta de una herramienta de software libre o manual de usuario, como soporte para capacitar al personal en el tema de seguridad, es otra problemática que enfrenta el Ministerio de Salud.

Es necesario, un plan de acción que ayude a la gestión del uso de la misma y a planificar la implementación de los software informático Nagios, OCS Inventory y la aplicación de normativas de seguridad basadas en la ISO 27001 que resuelvan las necesidades de información de la empresa, así como cualquier otro recurso, para lograr el cumplimiento de las metas y de los objetivos globales de la organización.

La propuesta de solución es desagregar la distribución laboral en las diferentes actividades del área de informáticas con sus respectivas fichas ocupacionales para ser incluidas al manual de funciones. Una alternativa para el mejoramiento de la red es la certificación de la normativa ISO 27001.

IV. JUSTIFICACIÓN

El Complejo Nacional de Salud "Dra. "Concepción Palacios" tal como lo hemos expuesto anteriormente no cuenta, con un manual de lineamientos de normativas para el resguardo y manejo de los recursos tecnológicos. Esto motiva a incorporar normativas de seguridad informática permitiendo la confiabilidad, integridad y disponibilidad en los equipos de cómputo, obteniendo beneficios en los servicios de red, satisfacción al usuario, eficiencia, reducción de costos, manejo excelente de las instalaciones y equipos, protección de los bienes de la empresa, procesamiento y asegurar la información, entre otras.

Es por eso, la importancia de este trabajo el proponer normativas de seguridad personalizadas y la integración del uso del software libre Nagios y el OCS-Inventory para monitorear los activos de cómputos conectados a la red LAN del Ministerio de Salud. Así se reducirán los riesgos y amenazas a los sistemas informáticos y sus componentes, optimizando y resguardando los equipos de comunicaciones que la institución debe proteger, logrando una buena administración al implementar estas herramientas.

Los beneficios de la propuesta de normativas seguridad ISO 27001 consisten en disponer de una metodología dedicada a la seguridad de la información reconocida internacionalmente; el puntualizar el proceso para evaluar, implementar, mantener y administrar la seguridad de la información; el diferenciarse en el mercado de otras organizaciones; la disminución de costos e inversiones; el formalizar las responsabilidades operativas y legales de los usuarios internos y externos de la información y el cumplimiento de las disposiciones legales ,entre ellas las leyes de protección de datos y privacidad entre otras.

Ventajas de tener una red administrada con Nagios.

Se puede monitorear los fallos en la red incluso antes de que los usuarios lo noten; controlar cada equipo y cada servicio de forma separada mediante una interfaz gráfica fácil e intuitiva; llevar un registro histórico de los fallos ocurridos

con un alto nivel de detalle, es decir cada equipo y cada servicio tiene asociado un historial de desempeño que facilita la labor del administrador y se podrá programar chequeos a equipos y servicios con previsión considerable.

Este proyecto será una guía, para que el MINSA proteja sus tecnologías informáticas basados en normativa de seguridad bajo la certificación de la ISO/IEC 27001. Habrá un giro de negocio análogo lo cual permitirá mejores práctica para la gestión de seguridad de la información en esta área tan sensible, el cómo estandarizar el proceso de implantación de la norma, garantizando la eficacia de los procesos establecidos con el fin de reducir los costos de gestión. Además, contará con un informe de lineamientos del hardware y el software conectados a red y la incorporación de las herramientas del software libre Nagios y OCS-Inventory para monitorear el tráfico de la red y el control del inventario.

V. OBJETIVOS

OBJETIVO GENERAL

1. Proponer normativas y estándares de seguridad Informática que contribuyan a la protección de los activos informáticos que enfrenta la red LAN del Complejo Nacional de Salud Dra. "Concepción Palacios".

OBJETIVOS ESPECÍFICOS

1. Realizar un diagnóstico de los sistemas de tecnología de hardware y software y del área de informática del Ministerio de Salud.

2. Evaluar los riesgos por escala cualitativa y cuantitativa para mitigar los peligro que afectan los activos de comunicaciones del Ministerio de Salud

3. Adecuar normativas y estándares de seguridad informática al contexto del Ministerio de Salud "Dra. Concepción Palacios".

VI. MARCO TEÓRICO

La seguridad de la información es la protección de la información de un rango amplio de amenazas para asegurar la continuidad del negocio, minimizar el riesgo y maximizar el retorno de las inversiones y las oportunidades comerciales.

Esta se logra implementando un adecuado conjunto de controles; incluyendo políticas, normativas, procesos, procedimientos, estructuras organizacionales, diagnósticos evaluación de riesgos y funciones de software y hardware. http://es.wikipedia.org/wiki/ISO/IEC_17799

La importancia de la seguridad de la información del sector público y privado, es proteger las infraestructuras tecnológicas tales como red, servidores de red, procesador, memoria, información, software y estaciones de trabajo.

1. Concepto de red

Las redes constan de dos o más computadoras conectadas entre sí y permiten compartir archivos y ejecutar aplicaciones de red.

2. Tipo de red

2.1 Red de Área Local (LAN)

La red local o LAN (Local Área Network) es un sistema de comunicaciones de alta velocidad que conecta microcomputadoras o PC y/o periféricos que se encuentran cercanos, por lo general dentro del mismo edificio.

Una LAN consta de hardware y software de red y sirve para conectar las que están aisladas y compartan entre sí programas, información y recursos, como unidades de disco, directorios e impresoras y de esta manera estarán a disposición de la información de cada puesto de trabajo y los recursos existentes en otras computadoras. http://es.wikipedia.org/wiki/Redes_Informáticas.

3. Características de las LAN's

1. Utilizan un medio privado de comunicación.
2. La velocidad de transmisión es de varios millones de bps.
3. Las velocidades más habituales van desde 1 hasta 16 Mbits, aunque se está elaborando un estándar para una red que alcanzará los 100 Mbps.
4. Pueden atender a cientos de dispositivos muy distintos entre sí (impresoras, ordenadores, discos, teléfonos, módems, etc.).
5. Ofrecen la posibilidad de comunicación con otras redes a través de pasarelas o Gateway.
6. Permite hasta 100.000 ficheros abiertos simultáneamente. El mismo servidor sirve de puente o Gateway con otras redes.

4. Ventaja de las redes

1. La Integración de varios puntos en un mismo enlace.
2. Posibilidad de que los PC's compartan entre ellos programas, información, recursos entre otros.
3. La máquina conectada (PC) cambia continuamente, permitiendo un proceso incremente sus recursos y capacidades.

5. Componentes de red

5.1 Servidor: Este ejecuta el sistema operativo de red y ofrece los servicios de conexión a las estaciones de trabajo.

5.2 Servidor de archivo: Almacena varios tipos de archivos y los distribuye a otros clientes en la red.

5.3 Servidor de impresiones: Controla muchas impresoras y acepta trabajos de impresión y realizan todas las funciones que en un sitio de trabajo se harán para lograr una tarea de impresión.

5.4 Servidor de correo: Almacena, envía, recibe, en ruta y realiza otras operaciones relacionadas con email para los clientes de la red.

5.5 Servidor de fax: Almacena, envía, recibe, en ruta y realiza otras funciones necesarias para la transmisión, la recepción y la distribución apropiadas de los fax.

5.6 Servidor de la telefonía: Realiza funciones relacionadas con la telefonía, como es, contestador automático con un sistema interactivo para la respuesta de la voz, almacenando los mensajes de voz, encaminando las llamadas y controlando también la red o el Internet, por ejemplo la entrada excesiva del IP de la voz (VoIP).

5.7 Servidor proxy: Realiza funciones a nombre de otros clientes en la red para aumentando el funcionamiento de ciertas operaciones; por ejemplo, depositar documentos u otros datos, sirve de seguridad por medio de Firewall. Permitiendo administrar el acceso a internet en una Red de computadoras.

5.8 Servidor del acceso remoto (RAS): Controla las líneas de módem de los monitores u otros canales de comunicación de la red para que las peticiones conecten con la red de una posición remota; responde llamadas telefónicas entrantes o reconocen la petición de la red y realizan los chequeos necesarios de seguridad y otros procedimientos necesarios al registrar a un usuario en la red.

5.9 Servidor web: Almacena documentos HTML, imágenes, archivos de texto, escrituras y material Web compuesto por datos conocidos colectivamente, el cual distribuye el contenido a clientes en la red.

5.10 Impresoras: Las impresoras son capaces de actuar como parte de una red de ordenadores sin ningún otro dispositivo, tal como un "print server", actúa como intermediario entre la impresora y el dispositivo que está solicitando un trabajo de impresión.

5.11 Estaciones de trabajo: Es la conexión de una computadora a una red, la primera se convierte en un nodo de la última y se puede tratar como una estación de trabajo o cliente. Las estaciones de trabajos pueden ser computadoras personales.

5.12 Tarjetas o Placas de Interfaz de Red: Es el proceso de conexión de un equipo a una red, el cual necesita de una tarjeta de interfaz de red que soporte un esquema de red específico, como Ethernet, ArcNet o Token Ring. Dicho cable de red se enlazara a la parte trasera de la tarjeta. También es conocida como adaptadores de red o sólo tarjetas de red. Este dispositivo obtiene la información de la PC, la convierte al formato adecuado y la envía a través del cable a otra tarjeta de interfaz de la red local.

6. Sistema de Cableado

El sistema de la red está constituido por el cable utilizado para conectar entre si el servidor y las estaciones de trabajo.

7. Recursos y Periféricos Compartidos

Los recursos compartidos incluyen los dispositivos de almacenamiento ligados al servidor, las unidades de discos ópticos, las impresoras, los trazadores y el resto de equipos que puedan ser utilizados por cualquiera en la red.

8. Administración de red

La administración de redes es un conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada con una planeación adecuada y propiamente documentada cuyos objetivos son:

- Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.

- Tener un uso eficiente de la red utilizando mejor el ancho de banda.
- Hacer la red más segura, protegiéndola contra el acceso no autorizado, haciendo imposible que personas ajenas puedan entender la información que circula en ella.
- Controlar cambios y actualizaciones en la red de modo que ocasionen las menos interrupciones posibles, en el servicio a los usuarios. www.monografias.com

8.1. Los elementos involucrados en la administración de red:

8.1.1 Agentes para coleccionar la información de administración del sistema en un nodo o elemento de la red. El agente genera el grado de administración apropiado para ese nivel y transmite información al administrador central de la red acerca de:

- Notificación de problemas.
- Datos de diagnóstico.
- Identificador del nodo.
- Características del nodo.

9. Administrador del sistema

Es el conjunto de programas ubicados en un punto central al cual se dirigen los mensajes que requieren acción o que contienen información solicitada por el administrador al agente.

Las operaciones principales de un sistema de administración de red son: las siguientes

9.1 Administración de fallas: Es la que maneja las condiciones de error en todos los componentes de la red, en las siguientes fases:

- Detección de fallas.
- Diagnóstico del problema.

- Resolución.
- Seguimiento y control.

Un administrador de red se encarga de asegurar la correcta operación de la red, tomando acciones remotas o localmente. Administrar cualquier equipo de telecomunicaciones de voz, datos y video, así como de administración remota de fallas, configuración rendimiento, seguridad e inventarios.

10. Administración de la red

La administración de la red será a través de Nagios, este es un sistema “open source” de monitorización de redes ampliamente utilizado, que vigila los equipos hardware y servicios software que se especifican, alertando cuando el comportamiento de los mismos, no sea el deseado.

Entre sus características principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP), la monitorización de los recursos de sistemas hardware, carga del procesador, uso de los discos, memoria, estado de los puerto, independencia de sistemas operativos, posibilidad de monitorización, remota mediante túneles SSL cifrados ó SSH, y la posibilidad de programar plugins específicos para nuevos sistemas.

Se trata de un software que proporciona una gran versatilidad para consultar prácticamente cualquier parámetro de interés de un sistema, y genera alertas, que pueden ser recibidas por los responsables mediante correo electrónico y mensajes SMS, cuando estos parámetros exceden de los márgenes definidos por el administrador de red.

Este software es llamado originalmente Netsaint, nombre que se debió cambiar por coincidencia con otra marca comercial, fue creado y es actualmente mantenido por Ethan Galstad, junto con un grupo de desarrolladores de software que mantienen también varios complementos.

Nagios fue originalmente diseñado para ser ejecutado en GNU/Linux/ Unix. Está licenciado bajo la GNU General Public License Version 2, publicada por la Free Software Fundation.

10.1 Descripción de monitoreo

- Monitorización de servicios de red (SMTP, POP3, HTTP, NTTP, ICMP, SNMP).
- Monitorización de los recursos de equipos hardware (carga del procesador, uso de los discos, logs del sistema) en varios sistemas operativos, incluso Microsoft Windows con los pluginsNRPE_NTóNSClient++.
- Monitorización remota, a través de túneles SSL cifrados o SSH.
- Diseño simple de plugins, que permiten a los usuarios desarrollar sus propios chequeos de servicios dependiendo de sus necesidades, usando sus herramientas preferidas (Bash, C++, Perl, Ruby, Python, PHP, C#...).
- Chequeo de servicios paralizados.
- Posibilidad de definir la jerarquía de la red, permitiendo distinguir entre host caídos y host inaccesibles.
- Notificaciones a los contactos cuando ocurren problemas en servicios o hosts, así como cuando son resueltos (a través del correo electrónico, buscapersonas, Jabber, SMS, o cualquier método definido por el usuario junto con su correspondiente complemento).
- Posibilidad de definir manejadores de eventos que ejecuten al ocurrir un evento de un servicio o host para resoluciones de problemas proactivas.
- Rotación automática del archivo de registro.
- Soporte para implementar hosts de monitores redundantes.

- Visualización del estado de la red en tiempo real a través de interfaz web, con la posibilidad de generar informes y gráficas de comportamiento de los sistemas monitorizados y la visualización del listado de notificaciones enviadas. http://es.wikipedia.org/nagios.org.

10.2 OCS Inventory

Se Implementará el software OCS – Inventory siendo una aplicación para el inventario de los PC's de la red, este procedimiento se realiza por medio de una estructura cliente servidor, el servidor Linux recopila la información que le envía un software agente instalado en cada uno de los pc's de Windows y Linux.Esta aplicación hace uso del protocolo TCP/IP al estar inter relacionado con la red.

El diálogo entre los equipos cliente y el servidor del OCS INVENTORY se basa en el protocolo de transferencia de hipertexto (HTTP) y el formato de los datos se hace en XML . El servidor de administración utiliza Apache , MySQL y Perl. OCS es multi-plataforma ya que se ejecuta bajo sistemas Unix , así como en Microsoft Windows. http://en.wikipedia.org/wiki/OCS_Inventory.

11. El Diagnóstico

Un diagnóstico, es una metodología para observar las técnicas de la administración de equipos de cómputos conectado a una red, explotar las debilidades de sus sistemas, recomendar cómo resolver o minimizar los problemas de seguridad de la información.

El diagnóstico de seguridad o evaluación de riesgos se define como el conjunto de metodologías y técnicas de instrucción aplicadas sobre un sistema determinado con el objetivo de conocer el nivel de seguridad informática real. http://www.monografias.com/técnicas-métodos-diagnostico-estado-seguridad/.

11.1 Pasos para la realización de diagnósticos:

- Se desea conocer la situación real de los sistemas y mejorarlos.
- Demostrar a la administración los riesgos existentes.
- Ayudar a la administración a dirigir los recursos a los sistemas más importantes y más vulnerables.
- Justificar la obtención de más recursos económicos.

12. Etapas metodológicas

1. Evaluación de Riesgos. Determina los resultados de vulnerabilidades de los riegos, a los que se enfrenta la organización en términos de tecnología.

2. Mitigación de los riesgos que afectan a los recursos tecnológicos, dada por la técnica de calificación cuantitativa para controlar la incidencia del evento malicioso.

3. Se adecuarán medidas de seguridad informática para el uso apropiado de los recursos tecnológicos.

Las normas de seguridad informática surgen como una herramienta organizacional, para enfatizar cada uno de los miembros de una estructura sobre la importancia y la sensibilidad de la información que favorecen al desarrollo y al buen funcionamiento institucional.

Estas medidas de seguridad surgen para evitar problemas y proteger los mecanismos de seguridad que se implementarán en los sistemas de redes de comunicación en cualquier institución. http://es.wikipedia.org/wiki/ISO/IEC_17799 Códigos de buenas prácticas de seguridad ISO/IEC 17799.

El estándar de seguridad informática ISO-27001:2005 es el único modelo aceptado internacionalmente para la administración de la seguridad de la información y aplica a todo tipo de organizaciones, tanto por su tamaño como por su actividad.

13. Implantación de un Sistema de Gestión

El documento "Implantación de Sistema a la Gestión de Información norma 27001, fundamenta a cerca del nivel de seguridad que presentan los sistemas de información y establece una técnica de mejoramiento permitiendo aumentar la seguridad en los activos críticos, reduciendo los peligros asociados con los sistemas de información y de red. www.wikipedia.org/wiki/ISO/IEC_27001/

El implantar un sistema de gestión de seguridad consiste en tener una visión sobre su nivel de seguridad, sugiriendo ayudar a solucionar los problemas de confianza que se detectan a diario con las futuras tecnología informática formulando normas de confianza para proteger los equipos de cómputos conectados a red.

Las soluciones para mejorar el nivel de confianza según el nivel de riesgo son:

1. Evaluar los riesgos que inciden sobre los activos conectado a red.
2. Definición de las normativas de seguridad.
3. Creación de un plan de gestión del sistema de la institución.
4. Definición de un marco de mejoramiento para los sistemas de red.

Las ventajas que ofrece esta normativa, es tener en cuenta que la seguridad al 100% no existe; pero, establece una técnica y medidas para mejorar la seguridad de los sistemas de red. Esta técnica se ve reflejada en una serie de primacías que se describen a continuación:

- Se retomará medidas contra incendio, datos a los sistemas, robos, falsificación, pérdidas, fallo, error, inconsistencia, virus informáticos, demora, saturación, escucha, acceso erróneo, respuesta errónea, atentado, catástrofe esta leyes reduce enormemente estas situaciones y garantizara identificar los riesgos que afectan a los activos de comunicación.

- La calidad se transforma en la seguridad como una actividad de gestión a los sistemas de información y comunicación.
- Impone la norma de seguridad, hasta la ejecución de los controles, el conjunto de acciones adoptadas reducirá al mínimo todo riesgo por robo, fraude, error humano intencionado o no, mal uso de instalaciones y equipo a los cuales está expuesto el manejo de información.
- Elabora un documento que proporcione los fundamentos básicos para administrar la seguridad de los activos conectados a red, basado en las normas internacionales. www.wikipedia.org/wiki/ISO/IEC_27001.

En este trabajo investigativo se logrará detectar la compatibilidad del sistemas de información y comunicación con respecto a la ISO/ICE 27001 y la necesidad de preservar, custodiar de manera adecuada las tecnologías de comunicaciones, Esto permitirá asumir la norma IRAM-ISO/ICE 27001, denominada Sistema de Gestión de Seguridad de la Información, debido a que es certificable bajo los esquemas nacionales de cada país.

14. DISEÑO METODOLÓGICO DEL TRABAJO MONOGRÁFICO

1. Tipo de investigación

La investigación a realizar se puede clasificar de diversas maneras atendiendo a la forma de especificarlas. En nuestro caso es ante todo una investigación de tipo cuantitativo ya que implica la evaluación de datos numéricos tales como cantidad de equipos, eficiencia de los mismos, sus características, su disposición física entre otros.

El trabajo investigativo fue desarrollado con el apoyo de autoridades y funcionarios del Ministerio de Salud Dra. "Concepción Palacios" Managua. Institución de carácter estatal que organiza, dirige y planifica a través de sus leyes en concordancia con las líneas general del estado, para que todos los nicaragüense tengan derecho a los servicios gratuitos de la salud.

2. Área de estudio

Es de carácter informático y en menor grado administrativo, ya que el objetivo básico es la Propuesta de normativas y estándares de seguridad informática para el uso adecuado de los activos de cómputo conectados a la red LAN del Complejo Nacional de Salud "Dra. Concepción Palacios."

3. Investigadores

Estudiantes egresados de la carrera de Ingeniería de Sistemas de la Universidad Nacional de Ingeniería.

4. Universo de estudio

El universo de estudio es proteger los equipos y servicios conectados a la red de área local del Ministerio de Salud, aplicando la normativa informática bajo el estándar ISO 27001.

5. Fuentes

Las fuentes de información son principalmente los usuarios de los equipos, es decir, los trabajadores que laboran en dicha institución, además de los responsables del área de Informática y las fuentes tomadas de internet.

6. Técnica de recolección de información a utilizar en la investigación

Dadas las características de nuestra investigación, las técnicas a utilizar para la recolección de la información son las siguientes:

- La observación directa.
- La entrevista

7. Aspectos a considerar.

7.1 ¿Qué observar?

7.2 ¿A quiénes observar?

7.3 ¿Para qué observar?

7.4 ¿Por qué observar?

7.5 ¿Quién observará?

7.6 ¿Qué clases de observación se llevo a cabo?

7.7 ¿Dónde observar?

7.8 ¿Qué instrumentos se utilizo para llevar a cabo la observación?

7.1 ¿Que observar?

Se observó el trabajo que llevan a cabo todos los empleados en las distintas dependencias de la institución, en especial el equipo informático que este opera; así como las instalaciones donde este se encuentra ubicado. Es decir todas las actividades de observación son centradas en los que sucede dentro de las instalaciones de la empresa a los componentes de la red.

7.2. ¿A quién o quiénes observar?

A los directores de las diversa aéreas, los empleados en el instante que realizan sus actividades que involucran uso del equipo de computo.

7.3. ¿Para qué observar?

Las finalidades de la observación es conocer el estado y la situación de los elementos de la que integran la red en cada una de las distintas aéreas del Minsa.

Para que corrijan o varíen las futuras acciones según los resultados que arrojen la observación. La observación dentro de la organización tiene como objeto reconocer la habilidad y el aprendizaje que tienen las actuaciones del empleado en el uso y manipulación de cada una de las estaciones de trabajo.

7.4. ¿Por qué observar?

Para recoger información y datos que permitan ver el funcionamiento y el medio en el cual se desarrollan las actividades.

7.5. ¿Quién observará?

- El estudiante interesado en el desarrollo del tema.

7.6. ¿Qué clases de observación se llevó a cabo?

La observación directa participativa en que el espectador realizo soportes técnicos relacionados con las tecnologías de hardware, recolectando la información que será procesadas en este estudio investigativo.

7,7. ¿Dónde observar?

Se observaron la interacción de los empleados en cada una de las distintas áreas de trabajo, con el equipo de cómputo.

7. 8. ¿Qué instrumentos se utilizó para llevar a cabo la observación?

Según la observación estructurada el instrumento que utilizamos fue la entrevista que facilitó la recolección de datos que permitió un diagnóstico informático.

8. Procedimiento de recolección de datos

- La entrevista directa al administrador de la red LAN
- Realización de soporte técnico para recolectar los problemas relacionados con la seguridad de los equipos de cómputos.
- Análisis cualitativo y cuantitativo para medir el grado del riesgo

Capítulo I. Diagnóstico de las tecnologías de hardware y software de la División de Sistemas de Información del Ministerio de Salud.

El diagnóstico de la situación actual del las tecnologías de hardware y software del área de informática del Ministerio de Salud, se llevó a cabo mediante un levantamiento físico realizado durante el mes de Agosto del 2008.

1.1 El procedimiento utilizado para realizar el levantamiento de la información fue el siguiente:

1. Se recopiló la información necesaria de cada PC, mediante visita de campos para llenar un formato por cada dispositivo y periféricos de conexión.
2. Se levantó un detalle del sistema operativo por cada equipo de cómputo.
3. Una breve descripción del funcionamiento de la administración del nodo-internet.
4. Conocer el funcionamiento real del área de informática y mejorarlo.
5. Estudio de viabilidad del proyecto.

El resultado de este análisis nos dará una visión clara sobre el equipo de cómputo existente y se podrá convertir en un documento de consulta para futuros proyectos de dicha institución.

Este estudio determina el grado de eficiencia u obsolescencia de los equipos informáticos para la implementación de una nueva y eficiente arquitectura de red.

El equipo computacional que conforma la red no solamente incluye las PC de escritorio, sino que comprende además aquellos dispositivos necesarios para la interconexión de los mismos, entre estos incluimos los Routers/Switch, servidores, impresoras, entre otros dispositivos.

El estudio se realizará de acuerdo a los parámetros establecidos, en el siguiente orden: analizaremos las computadoras de escritorio (PC), así como los diversos periféricos (impresoras), y luego procederemos a la exposición de los

equipos que permiten la interconexión de las PC (Switch/Routers, estructura del cableado).

El levantamiento de datos de los equipos de cómputo del Minsa arrojó como resultado la existencia de 572 computadoras (incluyendo PC de escritorio) También se incluyen 100 impresoras, 15 gabinetes.

1.2 Especificaciones técnicas de equipos informáticos

Se presenta las detalles técnicos de software, hardware, uso de correo, Internet/intranet, uso de equipos informáticos, cableado estructurado de la red y aplicaciones de bases de datos del Ministerio de Salud.

El área de informática utiliza la ficha de soporte técnico para el control del mantenimiento correctivo y atender a los usuarios con problema de su equipo asignado. La información del formato de solicitud de soporte técnico se traslada a la base de datos, para la presentación de informes estadísticos que solicitan las autoridades superiores. Ver Anexos # 1 pág.103.

1.3 Inventario físico de los equipos de cómputo

EL Ministerio de Salud cuenta con 752 equipos de cómputos conectados a red, 25 Switch Cisco Catalyst, 4servidores con las especificaciones siguientes:

- Servidor de correo e Internet Compaq, procesador. P IV, 512 RAM 60 GB DD.
- Servidor de desarrollo, Compaq, procesador. P IV, 512 RAM 132 GB DD.
- Servidor de respaldo, Compaq, procesador. P IV, 512 RAM 132 GB DD.
- Servidor Server B (aplicaciones), COMPAQ
- Procesador. P IV, 512 RAM 132 GB.

1.4 Inventario de software se clasifica en:

1.4.1 Software de uso genérico, son los programas de uso general y que están instalados en todas las computadoras de la institución. En la siguiente tabla el Ministerio de Salud lo representa así:

SOFTWARE	NOMBRE DEL SOFTWARE	LICENCIA
Sistemas Operativos	Windows 2000	NO
	Windows 2003	NO
	Windows 2007	NO
	Windows XP	SI
	Linux red had para los servidores Web	NO
Software de aplicación	Office 2003	NO
	Office 2007	NO
	Office XP	NO
Software de correo	Microsoft Outlook	NO
Software Antivirus	Symentec Corporativo 10.1	NO
	Kaspersky 6.0	NO

Tabla Nº 1.1 software de uso genérico en el Minsa Central

1.4.2 Software de aplicaciones

Están diseñados bajo plataforma Oracle Developer 6i y las Bases de Datos que están en la versión de Oracle 8i, SQL Server 2003, Access 2003, Visual. NET y Clíper, MS-dos, Visual Basic 6.0 con SQL Server 6.0 además de servicios web administrado con aplicaciones tales como apache, php y MySQl.

1.5 Sistemas operativos se clasifican en:

Los sistemas operativos utilizados siguen la línea Microsoft en sus diferentes versiones:

Sistema operativos	Cantidad de equipos
Windows vista	149
Windows 2007	95
Windows 2000	80
Windows 2003	100
Windows XP profesional	148

Tabla 1.2 Fuente propia

1.6 Hardware con el que cuenta la institución:

- Servidor de Desarrollo (Servidor Tipo A)
- Servidor de prueba y capacitación (Servidor Tipo B)
- Microcomputadoras para Desarrollo (Microcomputadoras Tipo A).
- UPS para cada Servidor (UPS Tipo A)
- UPS para cada computadora (UPS Tipo B)
- Estabilizadores para cada computadora y servidor (tipo a)
- Multifuncional (Impresora, fax, fotocopiadora).

La siguiente tabla presenta las especificaciones de los equipos de cómputos de escritorios y detalles técnicos de los servidores en uso.

COMPONENTES	ESPECIFICACIONES REQUERIDAS
COMPUTADORA DE ESCRITORIO	
Procesador	Intel Pentium con Tecnología de Doble Núcleo
Velocidad del Procesad	De al menos 3.40 Ghz
Bus del Sistema	Al menos 800 Mhz
Memoria Caché l2	Al menos 2MB
MEMORIA RAM	
Ranuras	Al menos 3 Ranuras PCI
Interfaces	1 paralelo, 1 gráfico, 1 teclado, 1 mouse, 1 serial, al menos 6 USB 2.0 ó 1 paralelo, 1 gráfico, 1 serial y al menos 8 USB 2.0
Video	Integrado, 256 MB independiente PCI Express
Audio	Integrado
Módem	Interno de 56 Kbps
Tarjeta de Red	De al menos 10/100 Mbps conector RJ-45
DISCO DURO	Disco duro de al menos 250 GB, SATA, 7200 rpm
Unidad Disco Flexible	3.5" de 1.44 Mb
Quemador de DVD y CD-RW	Al menos 16X/48X32X48X
MONITOR	Al menos 17" LCD (Flat Panel)
Mouse y Almohadilla	Incluidos
Teclado	En español
Parlantes	Externos
Protector Plástico	Para Monitor, CPU y teclado
Sistema Operativo	Microsoft Windows XP Profesional OEM en Español. Service Pack actualizado
Software de Oficina	Microsoft Office 2003 Estándar o superior en español OLP NL LoclGovt, con CD media incluido
Documentación	Manuales impresos y/o en CD
Certificación de Calidad de Fabricación	**ISO 9001 versión 2000, presentarlo vigente en su oferta**
Carta de Autorización del Fabricante y/o Distribuidor	Presentarla con fecha vigente en su oferta
Garantía de Fábrica	1 año en partes y mano de obra

COMPONENTES	ESPECIFICACIONES REQUERIDAS
CONECTIVIDAD	
Tarjeta de Red	Dos 10/100/1000 Mbps Ethernet Conector RJ-45
ALMACENAMIENTO	
Discos Duros	292 GB, Ultra 3 SCSI,15,000rpm, hotpliug, controlador RAID incorporado, al menos 4 discos de 73 GB cada uno
Tarjeta Controladoras	Tarjeta para RAID 5
Unidad de Discos Flexibles	3.5" de 1.44 MB
Unidad de Cintas de Respaldos	Con una capacidad de 160 GB/320 GB, con su tarjeta controladoras, incluido el software para respaldo compatible con el sistemas operativos
Cintas de Respaldos	10 cartuchos de formatos compatibles con la unidad de cinta (160 BG/320 BG)
CD-ROM	CD-RW/DVD Combo, Interno
OTROS	
Monitor	Pantalla Plana LCD de 17"
Mouse y Almohadilla	Incluidos
Teclado	104 Teclas en Español
ACCESORIOS	
Panel de luces de Diagnósticos	Panel de luces de diagnósticos para la identificación fácil y rápida de los componentes del servidor con fallas.
Análisis de predicción de fallas	Análisis de predicción de fallas incluidos para advertir cuando los componentes tales como abanicos, memorias, procesadores, discos duros, y fuentes de poder van a fallar.
Procesador de servicios y monitores	Procesador de servicios y monitores incluidos que provea información importante y monitores interno de la temperatura, discos duros y ventiladores y fuentes de poder.
Sistemas Operativos instalados	SO Windows Server 2003 Edición Estándar OLP NL LoclGovt con 5 licencias CAL, pre instalados y certificados. Software para el Encendidos/Apagado desatendido y programable, compatible con el sistema operativo solicitado.
Antivirus	Ultima versión compatible con el sistema operativo instalado, versión corporativa con 10 licencias de clientes.
Software administración de servidor e identificación de fallas	Incluidos.
Software para el Servidor	El software suministrados al equipo debe venir pre instalados de fabrica, debe ser original, en español, salvo previa presentación de constancias y debe tener su CD y manuales.
Documentación	Documentación pertinente impresa en papel y / o en medio magnético, como CD o discos 3 1/2".
Garantía de Fabricante	3 Años.

Tabla Nº 1.3 Especificaciones de los servidores.

1.7 Especificaciones técnicas de impresora

Modelo	Velocidad de impresión	Resolución de impresoras	Memoria de impresora	Interfaz de conexión
Lexmark Optra S 1855	18 ppm	1200 x 1200 dpi	-	Puerto paralelo
Hp Laserjet 1015	14 ppm	1200 x 1200 dpi	16 MB	USB
Hp Color Laserjet 2600n	Hasta 8 ppm	600x600 dpi	16 MB	1 USB, 1 Ethernet
Hp Deskjet 6940	36 ppm	1200 x 1200 ppp	32 MB	Ethernet i, USB, Pict Bridg
Epson fx-890	680 cps (12 cpi)	240 ppp x 144 ppp	128 KB	Paralelo, USB
Hp Laserjet 1320	21 ppm	1200 x 1200	16 MB	USB
Lexmark T520	20 ppm	1200 x 1200 ppp	264 MB	USB, paralelo bidireccional
Hp Laserjet p2015	27 ppm	1200 x 1200 dpi	32 MB	USB, Ethernet
Oki B6300	34ppm	1200dpi x 1200dpi	640 Mb	Ethernet ,USB
Epson fx-1180	455 cps (12 cpi)	-	32 Kb	Paralelo Bidireccional
Epson fx-2190	680 cps	240 x 144 dpi	128 KB	Puerto paralelo y USB
Epson LQ-2080	400 cps	360 x 360 dpi	64 KB	Puerto Paralelo

Tabla # 1.4 Especificaciones de impresoras

1.8 Descripción de la red LAN.

La ejecución del proyecto de reestructuración de la red LAN permitió que se agregaran un total de 752 puntos de red conectados a Internet y 15 gabinetes ubicados en el departamento de informática, edificio de biblioteca, primer nivel de atención, adquisiciones, Auditoría interna, Sigfa, financiero, Planificación, laboratorio, farmacia e infraestructura.

Tiene una topología de comunicaciones estrella conectados mediante Switch Catalys Cisco con tecnología de Fast Ethernet, especificación 802.3u 100 Mbps, posee una velocidad de 100 Mbps con cableado estructurado de tipo UTP CAT 5, con un ancho de banda de 2Gbps. El ISP (Internet Service Provider) es Alfanumérico. Dispone de una intranet con una velocidad de 10/100 mbps.

Durante el proceso de la entrevista se dejó entrever que, la División de Sistemas de Información no cuenta con un documento tecnológico institucional de normativas de seguridad ni está bajo un estándar la reestructuración de la red LAN. Poseen algunos lineamientos de seguridad en el uso de los equipos de comunicación y servidores, representando limitantes a la seguridad de los activos conectados a red. Ver anexo # 2 pág.104.

1.9 Administración de la red LAN

La administración de los puertos de red está a nivel de transporte de datos, el cual, se encarga de comunicar o enviar información de un equipo a otro, esto se logra mediante protocolo IP.

Actualmente, el direccionamiento IP es estático, el acceso a la red es controlado por el dominio de Internet, visualizando las aplicaciones que los usuarios llevan a cabo.

Se realizan configuración de cuentas electrónicas y se asignan permiso para el servicio de Internet a los usuarios con equipos de cómputos asignados por autorización de la Dirección del Ministerio de Salud.

Además, se aplican algunos lineamientos de seguridad para proteger los equipos de cómputos conectados a la red LAN, como la protección del cableado de red en tubo pvc; 12 gabinetes bajo llaves; la red está protegida por muros de fuegos en los sistemas operativos Windows y Linux y en un ambiente agradable a través ambiente climatizados.

1.10 Descripción del nodo de internet – Ministerio de Salud

El Ministerio de Salud cuenta con un nodo de Internet cuyo sistema operativo es red hat Linux release 9 (sheik), a una velocidad de 100 Mbps, aquí el nodo se administra con un único dominio minsa.gob.ni, que actúa como servidor de correo y servidor Web conectado a la red 10 SIGFA (Sistema Gerencial Administrativo Financiero) con el Ministerio de Hacienda y Crédito Público.

La institución dispone de un servidor de comunicaciones Cisco 2511 con 16 puertos de comunicación, el cual da acceso vía conexión dial-up a Internet y da cobertura a intranet para diferentes instituciones a nivel nacional.

1.11. Problemas de los sistemas de tecnologías de hardware y software

1. La infraestructura tecnológica de los sistemas de transporte de información no está sujeta a normativa.
2. El sistema eléctrico esta sobre saturado.
3. No poseen lineamientos de administración y gestión de los equipos informáticos ni de la administración de redes inalámbricas.
4. No cuentan con desarrolladores de bases de datos.
5. No posee una herramienta de software para la administración de la red de telecomunicaciones.

1.12 Alternativas de solución de las tecnologías de hardware y software

Se propone.

1. Proponer la reestructuración de sistema eléctrico apropiado a la plataforma tecnológica de red.
2. La implementación del software libre Nagios para la gestión de los dispositivos informáticos que permita una mejor administración en la identificación de problemas en todos cada uno de los equipos y servicios activos de red (Switch o conmutadores) que garanticen seguridad y fácil manejo.

3. Certificarse bajo el estándar de seguridad ISO/CEI 27001:2005 que les proporcionará los procedimientos de seguridad de la información reconocida internacionalmente.
4. Contratar desarrolladores informáticos para actualizaciones de los software hospitalarios y pagina web del Ministerio de Salud.

1.13 Análisis del área de informática (División de sistemas de Información)

La División de Sistema de Información está ubicada a un nivel de mando medio, ésta depende del área de División General de Planificación y Desarrollo, lo cual a su vez está bajo la Dirección Superior; solucionan los problemas relacionados con las nuevas tecnología computacional como normar los procedimientos del área de informática, funciones y flujos de los sistemas de información, formulan y actualizan los requerimientos de la información, así como el diseño y actualizaciones de las exigencia informáticas; supervisan el sistemas de información institucional y sectorial, administran y brindan mantenimientos a los sistemas de información. Existe un mantenimiento preventivo y correctivo al software y bases de datos que están en ejecución según la necesidad del usuario.

1.13.1 Problemas administrativos de la división de sistemas de información

La División de Sistemas de Información posee un desorden laboral por parte del personal ya que se ejercen tareas que no están contemplados con el cargo funcional; esto se debe a la rotación de personal que exiten en los puestos de confianza, como es la dirección de informática, este no es un cargo permanente. Tienen dificultad para ejecutar el control de las actividades relacionadas con los equipos conectados a red y conflictos para coordinar las funciones de cada puesto de trabajo.

Esta situación no les permitirá un desarrollo óptimo en las actividades relacionadas con sus tecnologías, por lo que, deberán modificar el área de informática e incluirlas en el manual de funciones de dicha institución.

Es necesario reconocer la gran importancia que tiene el análisis de la estructura organizacional en el proceso tecnológico, lo que está representa para la supervivencia de una institución del estado, con fines de mejorar la toma de decisiones.

La estructura organizativa es el esqueleto de todo sistema empresarial, representa los principios sobre las cuales la institución está constituida; cualquier falla, afecta la manera en que los subsistemas se comportan, pudiendo limitar el tipo de sistemas tecnológico que podrá en algún momento implementarse en la institución. Las primeras evidencias en este estudio, nos refleja que la organización forma parte del sistema tecnológico de la red LAN y su estructura actual puede perjudicarlo o apoyarlo.

El propósito de este análisis es reorganizar las funciones laborales de la División de Sistemas de Información, facilitando así una repuesta más eficaz a nivel laboral y tecnológico.

El análisis de los datos se llevaron a cabo, utilizando fuentes análisis documental, entrevistos y observación directa.

1.13.2 Organización funcional del Ministerio de Salud.

El enfoque establecido en el organigrama del Ministerio de Salud representa una autoridad de mando en la dirección superior, el consejo técnico y consejo nacional de salud del poder ciudadano son los encargados de aprobar todas las actividades que se desarrollan dentro de la institución y del buen funcionamiento de los servicios que prestan. Ver anexo # 3.Pag.110.

Existen cargos que ejercen funciones que no están contemplados con su perfil profesional, esto se debe a que los cargos son orientados por el gobierno.

Los responsables de cada división general y dirección general son responsables directo del buen funcionamiento de sus áreas laborales, éstos a la vez, rinden cuenta a la dirección superior mediantes informes generados por ellos.

Una parte de la estructura funcional del organigrama, donde está ubicada la División de Sistemas de Información, se observa que las funciones reflejadas allí son de carácter documental y tecnológico a nivel de relevancia, como un departamento, establecido por los sistemas de información para prestar servicio externo a través de los sistemas de comunicación en línea.

A partir de su misión y visión permitirá contar con el modelo estructural y funcional dentro de la organización, delimitando sus áreas funcionales, así como, los procesos y procedimientos técnicos administrativos de trabajo que le corresponderá desarrollar, con sus respectivos cargos y sus correspondientes perfiles ocupacionales.

Según los informáticos la División de Sistemas de Información refleja que hay una centralización excesiva de autoridad, demoras en la tomas de decisiones, dificultad en ejercer el control, rotación del personal, no cumplen con el perfil adecuado, dificultad para la coordinación entre funciones.

1.13.3 Propuesta de estructura organizacional departamento Informática.

Se desarrollará una estrategia para evaluar el área de informática y al personal, hasta alcanzar un nivel organizacional. El área de informática será analizada utilizando herramientas propias de las disciplinas aplicables; por ejemplo, se usará la organización del personal para los niveles de organización y personal.

En base a esto se propone desagregar los servicios que presta la división de sistemas de Información como un ordenamiento que ayudará a que exista una mayor facilidad de resolver o tomar las decisiones inmediatas. Tal como lo refleja en la figura siguiente:

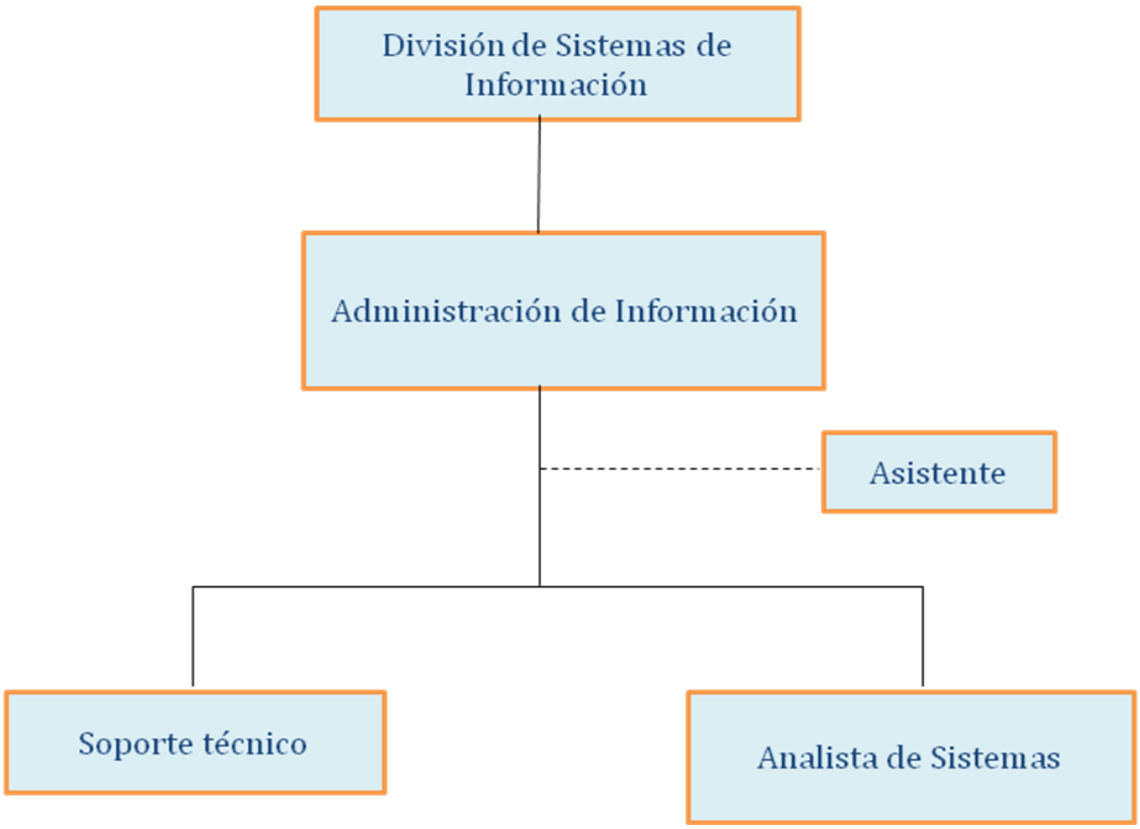


Figura N° 1.1 Propuesta de Estructura organizativa de la División de Sistemas de Información.

A continuación se detallan los diferentes principios que el Ministerio de Salud Dr. "Concepción Palacios" quiere alcanzar con una propuesta de estructura organizacional.

División del trabajo. Existencia de una buena división de trabajo que permita en cada Dirección Superior aprueba las actividades de programación, control y coordinación en materia de salubridad pública a nivel nacional.

Autoridad y responsabilidad. El organigrama debe reflejar claramente que entidades poseen autoridad y/o responsabilidad sobre otras.

Disciplina. Que existan responsabilidad en todas las divisiones y direcciones del MINSA, además están bien definidas.

- Unidad de mando. La unidad de mando está bien definida.
- Unidad de objetivos. Aunque existe un documento en el cual se han fijados los objetivos, leyes y metas institucionales, deben estar bien definidas.
- Jerarquía de autoridad. Que dentro del organigrama estén bien especificadas las autoridades superiores.
- Subordinación de los intereses individuales a los comunes. Los trabajadores de la salud se encuentren enfocado en garantizar el cumplimiento de la ley general de la salud y sus objetivos institucionales.
- Orden. El trabajador se encuentre en su puesto de trabajo, a si como sus herramientas necesarias para realizar sus funciones.
- Estabilidad en el cargo. Posean una estabilidad en su cargo lo que hace fácil el buen desempeño en sus labores o funciones.
- Iniciativa. El personal posea la iniciativa necesaria para el desempeño en sus labores.
- Equidad. Exista un trato de igualdad.
- Remuneración. El pago al funcionario sea lo justo por la labor que realiza de acuerdo al contrato firmado.

1.13.4 Característica del personal de la División de Sistemas de Información.

En toda institución la experiencia de los conocimientos que posea el personal es un factor indispensable para su éxito; así también el uso correcto de la tecnología de redes, internet y correo electrónico.

La preparación del personal debe cumplir con las siguientes generalidades

1. La identificación del personal a ser afectado por el cambio.
2. El análisis del manual de funciones actual por las partes involucradas.
3. La determinación de las funciones a ser agregadas, distribuidas o eliminadas.

1.13.5 Identificación del personal a ser afectado por el cambio

Se entiende que el personal de la División de Sistemas de Información serán los primeros afectados, ya que estos interactúan directamente con las Normativas de seguridad informática propuestas para las tecnologías. Entre sus están:

- Administrador de la red. Controla y monitorea las conexiones de toda la red e intranet del Minsa Central.
- Asistente. Su tarea dentro de la División de Información es la de operar la computadora, recibir las llamadas y e-mail de los usuarios que detectaron problemas informáticos en sus equipos de cómputos y entregárselos al administrador de la red; elabora el documento y realiza asistencia técnicas las divisiones que lo requiera.
- Soporte técnico. La función principal es la de realizar soportes correctivo y preventivos del sistemas operativos, ver los problemas de conectividad de la red, efectuar soporte preventivos a los equipos de cómputos y realizar diagnóstico de un equipo en mal estado para su posterior traslado al taller externo.
- Analistas de Sistemas. Se encarga de administrar la base de datos del Sistema de Información y garantizar su integridad y seguridad del hardware. Al final, de acuerdo al manual de funciones se harán las evaluaciones respectivas.

1.13.6 Manual de funciones actual por las partes involucradas

Aquí se especifica correctamente las funciones de los trabajadores, requisitos que tiene cada uno de los diferentes puestos de trabajo de la institución y se presentan los modelos de las fichas ocupacionales de los diferentes puestos de trabajo, ya que, la División de Sistemas de Información no lo tiene establecido.

Dichas funciones y tareas no se hallan de forma oficial o escrita, por lo que, sólo son conocidas por el empleado de forma privada, es decir, se le explica las actividades a realizar por puesto de trabajo, razón por el cual se proponen en la presente investigación la implementación del mismo.

Es a través de las fichas ocupacionales donde se hará la descripción de puesto o de tareas básicas que se desempeñan en el puesto de trabajo. El formato de la propuesta de la ficha ocupacional es la siguiente.

Ficha Ocupacional		
EMISION:	DIVISION	APROBADO POR:
DESCRIPCIÓN DE CARGO DE TRABAJO		
Dependencia Organizativa		
Nombre del Cargo		
Cargos Subordinados		
Propósito del Cargo		
FUNCIONES		
1		
2		
3		
4		
5		
Relaciones principales con otros Cargos		
Relaciones principales con otras Organizaciones y/o Instituciones		
Perfil del Cargo		
Conocimientos requeridos fundamentales		
Formación básica Nivel y especialización		
Conocimiento específico		
Conocimientos deseables		
Experiencia		
Otro requisitos		

Tabla # 1.5 Formato de fichas ocupacional

1.13.7 Determinación de las nuevas funciones agregadas y distribuidas

Esta fase comprende el desarrollo de las nuevas funciones y su distribución dentro de las actividades para cada uno de los involucrados en la propuesta de las normativas y estándares de seguridad tecnológico. No se va aumentar más trabajo, es decir, que solo se le establecerá un nuevo orden y responsabilidad.

Es necesario destacar que para la propuesta de las normativas de seguridad informática y la implementación del software libre Nagios, deben ser aprobadas por las autoridades de la institución y ser publicadas a nivel general.

A continuación se presentan las fichas ocupacionales de diferentes cargos funcionales, dentro de la estructura organizativa de la División de Sistemas de Información, a ser agregadas al manual de funciones del complejo Nacional de salud Dra. "Concepción Palacios". Ver anexo # 4, Pág.111.

1.14 Propuesta viabilidad del proyecto de certificación al Ministerio de Salud

La viabilidad es el análisis de un conjunto de necesidades para proponer una solución a corto plazo, tomando en cuanta restricción económica, tecnológica, legal y operativa. La permitirá a la institución proponer un documento tecnológico de normas de seguridad para los equipos de cómputos conectados a la red LAN, factible para su posterior aplicación y presentar un presupuesto para la realización del mismo. La oferta más óptima se aprobará de acuerdo al costo de inversión.

El MINSA cuenta con los recursos de software, hardware y comunicaciones necesarios para el buen funcionamiento del mismo. No obstante, parte de la tecnología es la forma en que el recurso humano hace uso de ésta y para ello es necesario un documento que guía este proceso, el cual actualmente no existe como tal. Esto conlleva a la necesidad de crear un manual sobre normativas de seguridad de la red y sus componentes tecnológicos referidos a equipos, accesorios, dispositivos varios, software y navegadores de internet, entre otros.

Las normativas servirán para mitigar los riesgos a los que están expuestos sus activos. Mediante ellas, se controlará el acceso a la red y se evitarán interfaces inadecuadas en la conexión. También habrá acceso al enlace de la red a los usuarios y se enviará el acceso de intrusos informáticos por medio de muros de fuego (firewall) a los servicios de comunicación.

1.14.1 Costo del proyecto

Para presentar la viabilidad del proyecto en las dos alternativas, se tomo en cuenta el costo de inversión del proyecto tales como: hospedaje, honorarios del auditor por mes, transporte, Alimentación, gasto varios de oficinas. Lo cual nos arrojo las siguientes opciones.

1. La contratación de un auditor nacional con un plan de trabajo de 6 meses cuyo costo aproximado será $1,000 (Mil dólares americanos).

2. La contratación del auditor internacional en la elaboración del Documento de Normativas con un valor aproximado de $35.000.00 (treinta y cinco mil dólares americanos).

Lo más viable para la institución es la inversión del menor costo puesto que se ahorra en pasajes aéreos y estadía en un hotel capitalino

Este estudio fortalecerá las aéreas informáticas de las entidades públicas del país, siendo el Ministerio de Salud Dra. "Concepción Palacios" el proyecto piloto de certificación bajo la norma ISO/IEC 27001.

Capítulo II. Evaluación de riesgos que inciden en los activos de cómputo conectados a la red LAN del "complejo nacional de salud "Dra. Concepción Palacios."

La evaluación de riesgos es el conjunto de metodologías y técnicas aplicadas sobre un sistema determinado con el objetivo de conocer el nivel de seguridad de los equipos y servicios conectados a red informática.

En este estudio se aplicará una evaluación de riesgos sobre los activos que están conectados a red, identificando sus peligros, frecuencias o probabilidad de de un evento destructivo y la magnitud del impacto para proveer una administración eficaz y sugerir medidas de seguridad para reducir losproblemas que actualmente enfrentan las comunicaciones del Ministerio de Salud considerando las siguientes acciones y actividades según el ISO 27001.

- Identificación de los activos que se deben proteger
- Identificar los problemas de la red.
- Detalles de los problemas actuales que afectan a los activos conectados a red LAN y propuesta de soluciones.
- Evaluación del riesgo, frecuencia e impacto frente a una escala con valores preestablecidos.
- Adecuar una herramienta para el monitoreo de los activos informáticos conectado a la red.
- Presentación de las normas informáticas que disminuyan los problemas informáticos.

2.1 Identificación de los activos a proteger en el Ministerio de Salud

2.1.1 Activos Físicos

1. Monitores
2. Switch de red
3. Red inalámbrica
4. Servidores de red
5. CPU
6. Teclados
7. Baterías
8. Estabilizador de voltaje
9. Mouse
10. Equipos ambientales
11. Memoria USB
12. Discos Duros portátiles

2.1.2 Activos de información

1. Datos de información de planos de la red
2. Cotizaciones para implementación de nuevos puntos de redes
3. Manuales de usuarios de planillas, inventario de activos de redes, insumos médicos
4. Licencia de software de Windows XP professional, Windows 98, Windows 2003, Windows 2000

2.1.3 Documentación en papel

1. Flujo gramas de soportes técnicos, manual de organización de soporte técnicos
2. Contratos de trabajos
3. Manuales de usuarios del software que están en uso
4. Constancias de ausencias
5. Permisos de trabajadores

2.1.4. Activos de software

1. Módulos hospitalarios, Oracle Developer 6i
2. Bases de datos de Módulos hospitalarios, Oracle 8i
3. Modulo administrativo SIAFI1, Idem
4. Software de control de soportes técnico
5. Software de insumos Médicos
6. Módulo de ATM, IDEM
7. Módulo de Compras y adquisiciones
8. Módulo de RRHH, IDEM
9. Sistemas de planificación(Sipla)
10. Producción de Servicios Consolidados
11. Módulos de cuadros de Gestión de producción de servicios
12. ATM Consolidados
13. Módulo de regulación de establecimiento de salud
14. Módulo de regulación de profesionales de la salud
15. Módulo de auditoría medica
16. Módulo de regulación de farmacias

17. Módulo de regulación de alimentos
18. Módulo de producción de servicios
19. Módulo financiero
20. Módulo de ATM
21. Cuadro de gestión
22. Programas ampliados de inmunizaciones
23. Sistemas informáticos de atención integral
24. Sistemas de captación de nominas
25. Sistema Integrado de programación y seguimientos de contratos
26. Sistema Nicaragüense de Vigilancia Epidemiológica Nacional
27. Programa comunitario de Salud y Nutrición
28. Epi- Info, es un programa de dominio público diseñado por el Centro
29. Control de Enfermedades de Atlanta (CDC) de especial utilidad
30. Sistema de Manejo de Suministros Humanitarios
31. Sistema Integrado de Gestión Financiera Administrativa y de Auditoria
32. Sistema de Vigilancia de mortalidad materna.
33. Sistema de Nómina Fiscal.
34. Sistema Nacional de Inversión Pública.
35. Programa de Inmunizaciones.
36. Software de S.O. y aplicaciones varias.
37. Bases de datos de atención a soporte técnico.

2.1.5 Activos de personal

1. Secretaria
2. Contadores
3. Administradores
4. Directores
5. Programadores
6. Usuarios de Planificación
7. Usuario de RRHH-Nómina
8. Usuario de Estadísticas, Epidemiología, farmacias, Adquisiciones,
9. Usuario de VIH-SIDA, Regulación, planificación, DGSS

2.1.6 Servicios de comunicaciones

1. Servicios de navegación por Internet
2. Servicios de correos
3. Servicio de mensajería instantánea.
4. Servicios soporte técnicos.

La información fue recopilada a través de las técnicas de la entrevista a los informáticos de la División de Sistemas de Información del Ministerio de Salud. Ver Anexo # 5 pág.119.

2.2 *Identificación de los riesgos informáticos que afectan a los equipos de cómputos conectados a la red LAN del Ministerio de Salud.*

1. Virus informáticos.
2. Conflicto IP.
3. Husmear conversaciones en líneas.
4. Robos de Equipos de Oficina.
5. Sustracción de Datos Confidenciales.
6. Fluctuación de energía eléctrica.
7. Inundaciones Provocadas por el Usuario.
8. Acceso no autorizado a las instalaciones de de la Red.
9. Tráfico de claves de información.
10. Conexión ilegal a la Red.
11. Falta de limpieza a los equipos de cómputos.
12. Daños a los sistemas operativos.
13. Acceso no autorizado a las bases de datos
14. Mal uso de la Internet y correo electrónico.
15. Falta de extintores contra incendios
16. Saturación de correo electrónicos
17. Acceso a la red inalámbrica
18. Saturación del ancho de banda
19. sabotaje informático

2.3 Análisis de los problemas y soluciones de la red LAN.

En este acápite se detallarán los problemas de la red y que afectan a la seguridad de los activos conectados a ella. Para ello, se tomó en cuenta las especificaciones de la norma ISO/ICE 27001 que alcanza el nivel de confianza deseado para lograr administrar la seguridad.

A partir de este análisis de los problemas de la red, se definirá una serie de lineamientos y estándares de seguridad que deberá alcanzar el nivel de seguridad deseado y acoplarlo al sistema de tecnología del Ministerio de Salud, mejorando el sistema de información como la protección del cableado, dispositivos de interconexión, hub, Switch, antenas inalámbricas para su mejor funcionamiento.

Los resultados del diagrama del problema y soluciones permitirán asegurar el acceso a los datos, recursos informáticos y gestionar los medios necesarios para administrar correctamente las tecnologías de comunicaciones de dicha institución.

En la tabla # 2.1 se refleja el diagrama de los problemas y soluciones de la red tomando como referencia la infraestructura, gestión de información y autenticación de la red del MINSA. Para ellos se presenta, un análisis de las dificultades de la infraestructura del nodo, la propuesta de solución y alcances para un mejor control sobre la tecnología.

Al medir los riesgos que afectan a los recursos informáticos se realizará por el método de cuantificación cualitativa y cuantitativa pasos que se retomaran a continuación.

2.4 Evaluación de riesgos informáticos a escala cualitativa

La valorización cualitativa son métricas asociadas con el impacto causado por la materialización de los peligros en la que se valoran los términos subjetivos como: alto, medio y bajo. Esta valoración estará asociada a un determinado nivel de impacto en función de multitud de factores como: Pérdidas económicas efectivas, pérdida de imagen de la institución entre otros. www.wikipedia.org/Análisis_de_riesgo_informático

El cuadro refleja la escala de calificación por la metodología cualitativa, tomando en cuenta nivel, impacto y la frecuencia o probabilidad de ocurrencia de un peligro informático, además de una breve definición del mismo.

NIVEL	IMPACTO	FRECUENCIA O PROBABILIDAD	DEFINICIÓN
3	Alto	Diario	El peligro está altamente motivado
2	Medio	Mensual	Cuando es posible que se dé un peligro.
1	Bajo	Anual	El peligro no posee la suficiente motivación

Cuadro Nª 2.1 Escala de calificación propuesta para medir el impacto del daño en la institución.

Aquellos activos que reciban una calificación de impacto alto (A) deberán ser objeto de atención inmediata por los encargados del área de informática del Ministerio de Salud.

Se presentan los pasos para la evaluación de los riesgos que afectan a los activos de red de la institución, son los que se muestran a continuación.

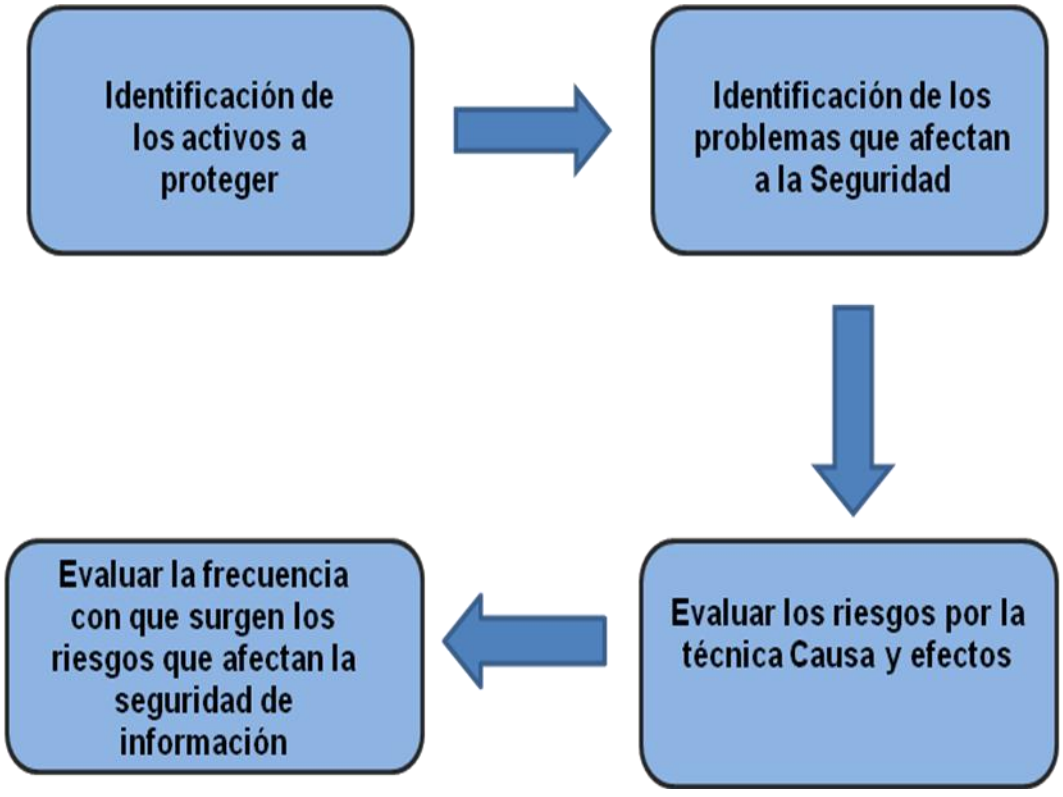


Imagen Nº 2.1 Pasos de una evaluación de Riesgos

Los resultados de esta evaluación de riesgos ayudarán a orientar y a determinar una adecuada implementación de controles para mitigar el peligro que inciden sobre los activos de redes, proponiendo lineamientos basados en las normas de seguridad para ser aplicadas en la red informática del Ministerio de Salud.

2.5 Matriz de riesgos aplicando el análisis de valoración cualitativo

La evaluación de riesgos valora los peligro, probabilidad de un evento e impacto sobre la plataforma tecnológica de la organización, con el fin de proponer lineamientos a un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la información. www.wikipedia/evaluacionde riesgos.com

También se tomará en consideración los activos que posee la información almacenada como: La red de datos, sistemas y usuario. Se propondrá técnicas que brinden seguridad lógica aplicando barreras y procedimientos para que resguarden el acceso de los datos y que solo permita acceder al personal autorizado.

De igual manera se evaluarán los problemas que afectan a la seguridad de los equipos de cómputos conectados a red LAN, como son:

- ✓ Usuarios
- ✓ Programas maliciosos
- ✓ Intruso informáticos
- ✓ Red de datos
- ✓ Sistemas

La tabla # 2.2 presenta la matriz de riesgos determinando las causas, efectos e impacto de los peligros que generan daños a los activos de redes del Ministerio de Salud; estos riesgos fueron obtenidos por la observación directa, reportes e información presentada por el administrador de la red y soportes técnicos de los problemas físicos y lógicos de los equipos de cómputos conectados a red.

2.6 Análisis de las frecuencias e impacto de los riesgos informáticos que afecta la red LAN del Ministerio de Salud.

1. *La Probabilidad*, es la conceptualización o la aparición de un riesgo que *pueda afectar a los activos de redes o sistemas de información.*
2. *El impacto*, es la medición y valoración del daño que podría producir a la organización un incidente de seguridad.
3. *La severidad* del riesgo se da cuando los eventos negativos en contra la seguridad en la red, ocasionan pérdidas monetarias a la institución.

En el caso de la conexión de red LAN y la red Inalámbrica del MINSA, se realizó una valoración de cada problema de seguridad, proponiendo una media ponderada para ajustar los resultados en la que se calificará cada riesgo informático, obteniendo una cifra para cada uno de los siguientes grupos:

- Frecuencia o probabilidad
- Impacto

La escala de calificación utilizada en este análisis está detallada en el cuadro Nº 2.1 del presente documento. Se presentan el nivel del riesgo que afectan la seguridad de los sistemas informáticos los cuales se detallaron en base a su frecuencia e impacto. A través de esta dinámica utilizamos el procedimiento para valorar la frecuencia e impacto para ellos se deben en listar las causas que generan el riesgo, la valoración de la frecuencia y el impacto que ocasiona los problemas informáticos a la red del Ministerio de Salud. Este proceso se llevó a cabo en conjunto con el apoyo de los ingenieros de la División de Sistemas de Información del Ministerio de Salud**.**

CAUSAS	RIESGOS	FRECUENCIA	IMPACTO
Fluctuación de energía eléctrica por cableado sobre cargado	Pérdida de los servidores	Anual	B
Problema del cableado eléctrico y daños intencional por parte del usuario.	Daños y pérdida del activo	Cada 6 meses	B
Usuario no capacitado en el uso de equipos de cómputos.	Desconocimiento informático	Diario	A
Virus informáticos, pérdida de los discos duros, daños al CPU, USB, diskette.	Pérdidas de datos	Cada 4 Meses	A
Perdida de servidor de aplicación y de disco duros portátil.	Pérdida de copias ce resguardo	Cada 2 Meses	B
Intrusos maliciosos, daños provocados por golpes, Etc.	Memorias USB, discos duros Portátiles	Diario	A
Caída de los servicios de comunicación.	Servidores de correos saturados	Diario	A
Switch inalámbrico sin medidas de seguridad.	Acceso no autorizado a las instalaciones de La Red (área de informática).	Diario	A
Acceso a páginas con amenazas de virus, compartir carpetas por el Messenger y en la red, uso de USB, perdida de la información.	Virus informáticos	Diario	A
Conflicto de direcciones IP.	Pérdida de conexiones a la red	Cada 3 meses	M
Robos mal intencionados por falta de control de seguridad.	Pérdida de imagen de la institución	1 vez al año	B
Husmear conversaciones en líneas	Delito contra la intimidad del usuario	2 veces al año	M
Extinguidores Contra Incendios Dañados	Incendios	1 vez al año	M
Falta de un control administrativos.	Humedad	Cada 3 Meses	M
Fluctuación de energía eléctrica, daños a los electrodomésticos de la institución y equipos de cómputos.	Cableado eléctrico saturado	Diario	A
El equipos se reinicia constantemente, problema de arranque y virus informáticos	Pérdida de los sistemas operativos	Anual	M

Tabla Nº 2.3 Análisis de las Frecuencias e Impacto de los riesgos de los activos de la red

2.7 Propuesta de un instrumento de medición por calificación cuantitativa

Un modelo cuantitativo es aquel en el que las consecuencias de la materialización de riesgo se asocian a un determinado nivel de impacto en función de la estimación del costo económico que conjetura para una organización.

El análisis de riesgo cuantitativo se ocupa específicamente de la revisión de la cantidad de riesgos determinando numéricamente la frecuencia de ocurrencia de una eventualidad, el impacto económico del daño producido.

Para mitigar los riesgos que inciden en los equipos tecnológicos se realizara el cálculo del valor del impacto promedio por la probabilidad de ocurrencia un activo de cómputo, tomado como referencia los datos del cuadro # 2.1 escala de calificación cualitativa donde se define la continuidad directa al número de veces que el evento puede ocurrir en un periodo de un año y la probabilidad que se dé un incidente sobre un activo es del 0% al 100% de certeza. La magnitud del riesgo es proporcional a la frecuencia con que ocurren los eventos.

Para valorar el grado de magnitud de un riesgo informático, se hará por la siguiente fórmula matemática.

Riesgo Total= Probabilidad de Amenaza x Impacto (Magnitud del Daño).

Para la presentación del resultado (riesgo) se usa una gráfica de dos dimensiones, en la cual, el eje-x (horizontal, abscisa) representa la "Probabilidad de Amenaza" y el eje-y (vertical, ordenada) la "Magnitud de Daño". Datos detallados en la matriz de riesgos por calificación cuantitativa. A partir de esta fórmula determinaremos su tratamiento y aplicar los controles de seguridad informática.

Para calcular la probabilidad de cada evento se realizo una regla de tres, tomando la frecuencia en la que aparece un riesgo en un periodo de 1 año.

1año ——————— 365 días

X ——————— 1 vez al año

X= 1/365= 0.0027*100%= 0.27%

- La magnitud del riesgo es proporcional a la frecuencia con que ocurren los eventos.
- La frecuencia con que ocurren los eventos es proyectada al año que equivalente a 365 días.

ITEMS	NIVEL	IMPACTO	EVENTOS (FRECUENCIA) ANUAL	PROBABILIDAD ANUAL (0% a 100%)	RIESGO TOTAL POR EVENTO
1	**2**	B	**1** año	0.27	0.27
2	**2**	B	**2** veces al año	0.55	0.55
3	**3**	A	**365** días	100.00	100.00
4	**3**	A	**3** veces al año	0.82	0.82
5	**2**	B	**6** veces al año	1.64	1.64
6	**3**	A	**365** días	100.00	100.00
7	**3**	A	**365** días	100.00	100.00
8	**3**	A	**365** días	100.00	100.00
9	**3**	A	**365** días	100.00	100.00
10	**2**	M	**4** veces al año	1.10	1.10
11	**1**	B	**1** año	0.27	0.27
12	**2**	M	**2** veces al año	0.55	0.55
13	**2**	M	**1** vez al año	0.27	0.27
14	**2**	M	**4** veces al año	1.10	1.10
15	**3**	A	**365** días	100.00	100.00
16	**2**	M	**1** año	0.27	0.27

Tabla # 2.4 Matriz de riesgo por calificación cuantitativa

Gráfico de la magnitud del riesgo por escala cuantitativa

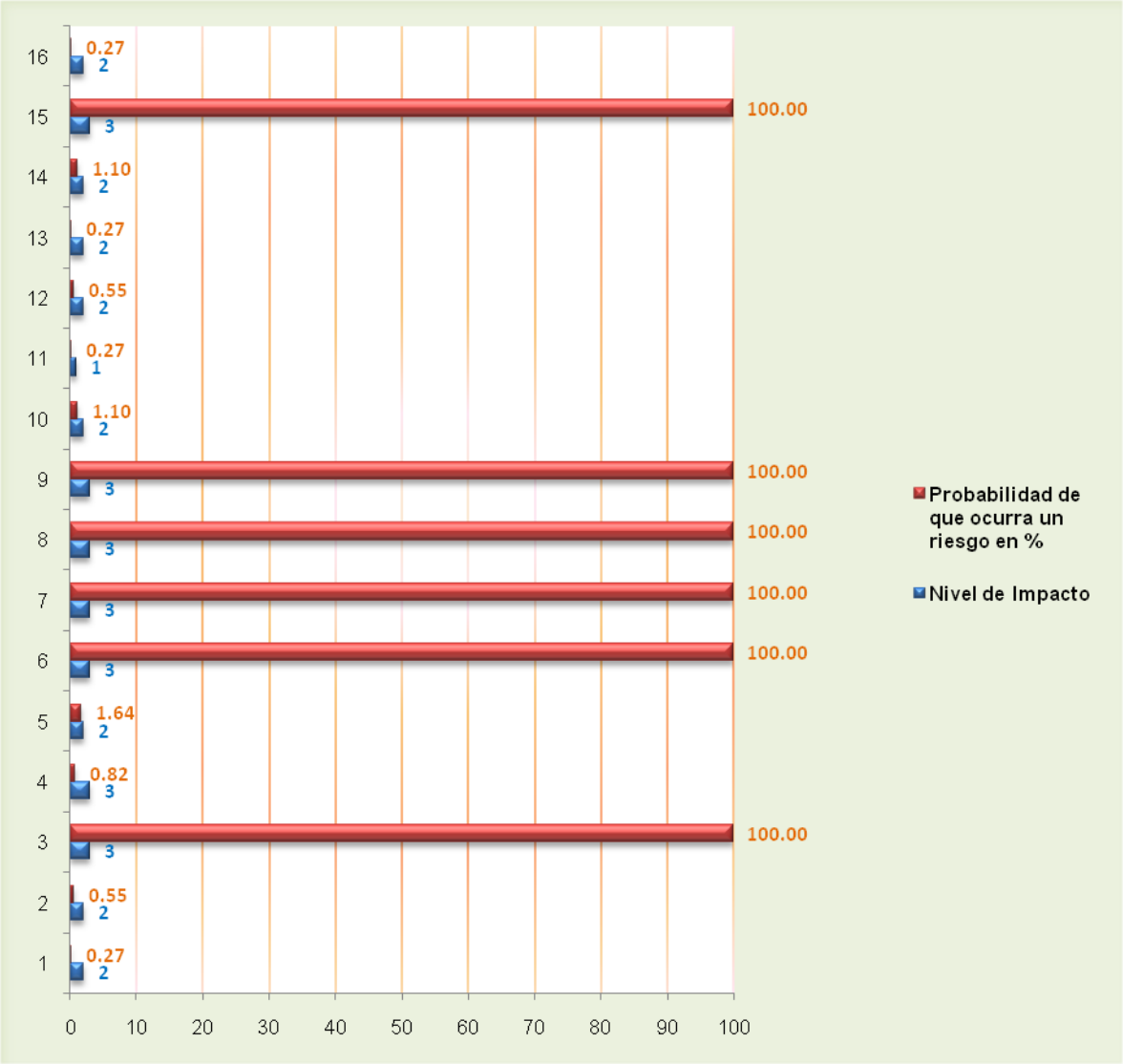


Imagen # 2.2 Grafico de magnitud de riesgos

En el eje de las ¨X¨; se cuantifican las probabilidades (en %), de ocurrencia de cada uno de los eventos, independientemente de que estos ocurran de manera aislada.

En el eje de las ¨Y¨; se ubican los Niveles de Impactos para cada uno de los eventos mencionados en la tabla # 2.4 Matriz de riesgo por medición cuantitativa.

Al evaluar los riesgos que afectan a los elementos del sistema y plataforma tecnológica del Ministerio de Salud, se propondrán normativas y estándares de confianza que aseguren un ambiente informático, bajo los criterios de confidencialidad, integridad y disponibilidad de la información tomando en cuenta los elementos del sistema:

- El software.
- Líneas de comunicación.
- Las aplicaciones del sistema.
- Datos

ELEMENTO	*CONFIDENCIALIDAD*	*INTEGRIDAD*	*DISPONIBILIDAD*
Software	Realización de copias no autorizadas el software.	Alteración de los programas en funcionamiento, haciéndolo fallar en el momento de su ejecución.	Eliminación de programas denegando el acceso a los usuarios.
Aplicaciones del sistemas	Uso sin autorización un equipo informático	Usurpación de la información almacenada en los equipos conectados a la red.	Robos y sobrecargas de corriente eléctricas por equipos de cómputos.
Datos	Lectura de datos no autorizados.	Modificación de los archivos confidenciales	Eliminación de archivos denegando el acceso a los usuarios
	Revelación de datos ocultos de manera indirecta		
Líneas de comunicación	Lectura de mensajes.	Mensajes modificados	Destrucción o eliminación de masajes
	Lectura de Chat.		

Cuadro N° 2.2 Elemento del sistema que afectan a la seguridad.

Para que estos sistemas estén protegidos de los peligro, se aplicarán normativas de seguridad a las áreas y recursos más sensibles que asigna la norma ISO/ICE 27001 tomando en consideración los siguientes aspectos.

- Normas de seguridad física y lógica.
- Respaldos y medidas de recuperación;
- Normas para el control de usuarios.
- Normas de acceso a la red LAN.
- Normas de acceso a Internet.
- Normas de seguridad de correo electrónico.
- Normas de seguridad de acceso remoto.
- Normas de uso de recursos informáticos.
- Normas de seguridad a los programas informáticos.etc

En base al análisis de las frecuencias e impacto y evaluación de los riesgos que amenazan a la seguridad de la red, permitió plantear alternativas para administrar las tecnologías informáticas en un ambiente seguro tal como la utilización de un software libre para administrar los equipos y servicios conectados a red y un documento de lineamientos de seguridad basado en el planteamiento de la normativa ISO 27001.

Los beneficios de esta metodología de administración son:

1. Identificación de riesgos que requieren mayor atención y áreas críticas.
2. Propuesta de alternativas como normativas de seguridad.
3. Permite la intervención inmediata y la acción oportuna de un riesgo.
4. Evaluación metódica de los riesgos.
5. Promueve una sólida gestión de riesgos en las instituciones.
6. Monitoreo continuo de un software de seguridad.

Se realizará un análisis de los diferentes software libre tales como: Pandora, OpenNMS, Zabbix, Zenoss y Nagios y proponer una interfaz web como herramienta para administrar los equipos y servicios que están expuestos a problemas que surgen fuentes no fiables como es el enlace de punto.

2.8 Análisis de las alternativas del software Pandora, Open NMS, Zabbix, Zenoss y Nagios para administrar la red.

2.8.1 Software libre Pandora

Es un software libre que permite analizar de forma visual, utilizando un navegador, el rendimiento y estado de algunos parámetros de diferentes sistemas operativos, servidores, aplicaciones y sistemas hardware como: Firewalls, Proxies, Bases de Datos, Servidores Web o Routers. Todo ello integrado en una arquitectura abierta y distribuida.

En esta herramienta proporciona agente para cada plataforma. Pandora puede monitorizar sistemas hardware con pila TCP/IP, como balanceadores de carga, routers, Switch o impresoras.

2.8.1.1 Las características específicas Open Source:

- Detección automática de la red y detección de topología
- Rendimiento y disponibilidad de seguimiento.
- Fallo y Gestión de Eventos.
- es un software de multiplataforma para Windows, HPUX, Solaris, BSD, AIX y Linux.
- Alta Disponibilidad.
- Monitoreo SNMP.
- Supervisión del filtro de SNMP.
- Elaboración de informes.
- Monitoreo por Internet.
- Inventarios.

Las pruebas programadas de la disponibilidad del monitoreo son:

1. ICMP de respuesta y demora
2. SNMP respuesta
3. TCP / IP estándar de servicios (HTTP, SMTP, etc.)
4. Especificado puertos TCP / IP
5. Disponibilidad de los servicios de Windows
6. Windows disponibilidad del proceso
7. Linux / Unix proceso de disponibilidad
8. URL disponibilidad
9. Nagios Plug-In de apoyo (para los dos, la disponibilidad y el rendimiento)

2.8.1.2 Requerimiento mínimo de software y hardware

1. Memoria RAM: 512 MB
2. Espacio de disco: 200 MB
3. Sistema Operativo: Windows Server estándar edición 2003

2.8.2 Software OpenNMS

Es una empresa de grado de supervisión de red y gestión de red desarrollada en el marco del software libre o código abierto del modelo.

2.8.2.1 Características del OpenNMS

- Determina la disponibilidad de los servicios, como la medición distribuida de disponibilidad y latencia, y presentación de informes sobre los resultados.
- La recolección de datos - la recogida, almacenamiento y presentación de informes en los datos obtenidos a través de protocolos, incluyendo nodos SNMP , JMX , HTTP, Windows Management Instrumentation , y NSClient.

- Umbral - la evaluación de los datos consultados latencia o recogidos los datos de rendimiento contra los umbrales configurables, la creación de eventos cuando estos se sobrepasen o rearmados
- Gestión de eventos - eventos que reciben, tanto internos como externos, entre ellos a través de traps SNMP
- Alarmas y automatizaciones - reducción de los eventos de acuerdo con una clave de reducción de secuencias de comandos y acciones automatizadas en torno a las alarmas
- Notificaciones - transmisión de los anuncios sobre acontecimientos dignos de mención por e-mail, XMPP , u otros medios.

2.8.2.2 Plataforma compatible.

La base de datos está escrita principalmente en Java, que en teoría puede funcionar en cualquier sistema que soporte un 1.5 MHz o superior.

2.8.2.3 Requerimiento mínimo de hardware y software

1. Memoria RAM: 512 MB
2. Espacio de disco: 200 MB
3. Sistema Operativo: Windows 2003 o superior, Linux, solaris
4. PC Pentium II o superior

2.8.3 Software zabbix

Es una herramienta de monitoreo de redes que permite gestionar los datos, esta herramienta permite desplegar gráficos, datos y mapas, además de realizar la configuración de la herramienta vía Web y notificar la ocurrencia de eventos predefinidos.

Zabbix cuenta con documentación con foro y listas de correo que hacen posible intercambiar experiencias con usuarios, herramienta que permite solucionar de una manera más rápida, realizar sugerencias, reportar fallos de la herramienta y publicar parches para algún caso en particular.

2.8.3.1 Requerimientos de zabbix

1. Corre sobre *Linux*
2. Requiere *Apache*
3. Bases de datos Mysql

La base de datos de *Zabbix* permite el manejo de usuarios y grupos de usuarios de la herramienta, equipos y grupos de equipos gestionados, variables a monitorear, disparadores de eventos, alertas, alarmas, acciones cuando se producen eventos, datos históricos de las variables monitoreadas, mapas ,gráficos, entre otros aspectos.

La interfaz Web es muy amigable y permite escoger el grupo de equipos, el equipo gestionado y diferentes opciones para visualizar los valores de variables en forma textual o en un gráfico, los monitoreo diario de correo electrónico, placa de interfaz y conexiones telefónicas está activo, y además permiten enviar la información del sistema

2.8.3.2 Requerimientos mínimos de software y hardware

El hardware va a depender proporcionalmente a la cantidad de dispositivos o hosts a monitorear, y el tiempo de los históricos que deseamos almacenar en nuestra base de datos: Se recomienda un Pentium II 350 MHz y 256 MB de RAM, para aproximadamente 20 hosts monitoreados, y un espacio de Disco duro de 6,5 GB para el almacenamiento de históricos por un año, para esta misma cantidad de hosts.

2.8.4 Software Zenoss

Es una aplicación de informática de código abierto, plataforma para la gestión de red y servidores basada en el servidor de aplicaciones Zope. Liberado bajo la Licencia Pública General de GNU (GPL) versión 2, Zenoss Core provee una interfaz web que permite a los administradores de sistemas monitorear disponibilidad, inventario/configuración, desempeño y eventos.

Zenoss Core combina programación propia y de varios proyectos de código abierto con el fin de integrar el almacenamiento de datos y los procesos para su recolección en una interfaz de usuario orientada a web. Se basa en las siguientes tecnologías de código abierto:

- Servidor web orientado a objetos desarrollado en Python
- Lenguaje de programación extensible
- Protocolo de monitoreo que recolecta información sobre el estado de los sistemas.
- Grafica y guarda registros de series temporales de datos en RRDtool
- Motor de base de datos muy popular de código abierto en MySQL
- Herramienta para interconexión de redes dirigida por eventos desarrollada en Python.

2.8.4.1 Funcionalidades

- Monitoreo de disponibilidad de dispositivos en la red utilizando SNMP
- Monitoreo de servicios de red (HTTP,POP3,NNTP,SNMP,FTP)
- Monitoreo de recursos de máquinas anfitrionas (Microprocesador, utilización de disco) en la mayoría de los sistemas operativos de red.
- Monitoreo de rendimiento de dispositivos a través de series temporales de datos
- Monitoreo Windows Management Instrumentación utilizando SAMBA y las extensiones de código abierto de Zenoss
- Herramientas de gestión de eventos para anotar las alertas de un sistema

- Detecta automáticamente recursos en una red y cambios en su configuración
- Sistema de alertas que provee notificaciones basadas en un conjunto de reglas y calendarios
- Soporta el formato de plugins Nagios

2.8.4.2 Requerimiento de hardware y software

1. 128 Mb de memoria RAM
2. Procesador 2 G Hertz
3. 200 MB Disco Duro

2.8.5 Software Nagios

NAGIOS es un sistema de monitorización de redes ampliamente utilizado para vigilar los equipos hardware y servicios software, alertando cuando el comportamiento de los mismos no sea el deseado.

2.8.5.1 Característica de Nagios

- Muestra un croquis del monitoreo
- Muestra un detalle de los equipos y servicios con problemas
- Detalla la información de cada equipo monitoreado
- Descripción de los problemas de equipos y servicios
- Herramientas Sin costo
- Análisis y estadísticas de tráfico de red
- Monitoreo de recursos de Servidores
- Detección de identidades de usuarios de la red
- Notificación de contacto.

Este software es una interfaz web sencilla que permitirá ver el status actual de la red LAN, realizar reportes de disponibilidad de los servicios de internet y proporcionará al administrador de los servidores del Ministerio de Salud gran cantidad de acciones como el conocer los problemas que ocurren en la infraestructura del nodo, monitorear el ancho de banda, controlar los puertos,

Switch, servidores y PC, además suministrará algunas acciones de seguridad tales como:

- Monitorear los servicios de red (SMTP, POP3, HTTP, NTTP, ICMP, SNMP).
- Monitorear los recursos de equipos hardware (carga del procesador, uso de los discos, log del sistema) en varios sistemas operativos, incluso Microsoft Windows con los plugins NRPE_NTó NSClient.
- Monitorear remotamente, a través de túneles SSL cifrados o SSH.
- Diseñar los plugins, que permitieran a los usuarios desarrollar sus propios chequeos de servicios dependiendo de sus necesidades, usando sus herramientas preferidas (Bash, C++, Perl, Ruby, Python, PHP).
- Chequea los servicios paralizados de la red.
- Posibilidad de definir la jerarquía de la red, permitiendo distinguir entre host caídos y host inaccesibles.
- Notificar los contactos cuando ocurren problemas en servicios o hosts, así como, cuando son resueltos (a través del correo electrónico, buscapersonas, Jabber, SMS, o cualquier método definido por el usuario junto con su correspondiente complemento).
- Posibilidad de definir manejadores de eventos que ejecuten al ocurrir un evento de un servicio o host para resoluciones de problemas proactivas.
- Rotación automática del archivo de registro.
- Soporte para implementar hosts de monitores redundantes
- Visualización del estado de la red en tiempo real a través de interfaz web, con la posibilidad de generar informes y gráficas de comportamiento de los sistemas monitorizados, listado de notificaciones enviadas, historial de problemas y archivos de registros.

2.8.5.2 Beneficios para administrar los equipos y servicios conectados a la red LAN del Ministerio de Salud en la plataforma del software Nagios.

- Libera a los administradores de realizar chequeos periódicos a determinados servicios críticos.
- Alerta sobre las pérdidas de servicio.
- Mayor personalización.
- Utilización de estándares.
- Interfaz gratuita
- Permite analizar y diagnosticar problemas de red.
- Avisa de los problemas antes de que los usuarios empiecen a quejarse.
- No requiere inversiones en Hardware, software e integración, ni personal especializado.
- Antes de realizar la instalación de Nagios en Debían se deben tomar en cuentas las siguientes exigencias.
- Tener una máquina con Linux y configurado TCP/IP ya que muchos servicios se revisan mediante esta función.
- Tener un servidor web y configurarlo con apache2.
- Un compilador GCC y GDD para soportar el mapa de estado de la red.
- Tener instalado la librería rdtool que proporcionará la base de datos para generar los gráficos básicos de la red.
- Tarjeta de red activa en el equipo.

2.8.5.3 Requerimientos de hardware pre-instalación de Nagios

1. El espacio en Disco duro debe ser mayor de 80 G
2. Memoria RAM de 512 como mínimo
3. Procesador de 2. G Hertz
4. Una unidad de CD o DVD para la instalación del sistema operativo.

2.9 Alternativas software de administración de red

NOMBRE DEL SOFTWARE	CONECCION A BASES DE DATOS	MEMORIA	PROCESADOR (DISCO DURO)	SEGURIDAD	SISTEMAS OPERATIVOS
PANDORA	JAVA	512 MB	200 MB, 3 G Hertz	Conteo relativos de fallos de seguridad	Windows Server estándar edición 2003 o superior, Fedora, Debían Lenin
OPENNMS	JAVA	512MB	200 MB, 2 G Hertz	Acegi de seguridad para manejar la autenticación y la autorización para la web app	Windows 2003 o superior. Linux
ZABBIX	JAVA	128 MB	200 MB 3 G Hertz	Supervisión de las actividades de la red	Windows 2003 o superior. Linux
ZENOSS	JAVA	128 MB	200 MB, 2 G Hertz	Vigilancia de la disponibilidad de dispositivos de red	Windows 2003, Linux ,Unix, java
NAGIOS	Lenguaje C php y perl	512 MB	80 G, 2. G Hertz	Sistemas de alarmas	Apache, Windows 2007, ,java, Linux

Tabla # 2.5 Alternativas de software de monitoreo de red.

En este estudio se logró detectar las alternativas de implementación de las diferentes herramientas de monitoreo como Pandora, opennms, Zabbix, zenoss y Nagios, con el objetivo de preservar, custodiar de manera adecuada las tecnologías de comunicaciones para ser aplicada a los recursos tecnológicos del Ministerio de salud.

Así mismo hay que destacar que los software de monitoreo de TI OpenNMS, zabbix, zenoss y pandora es programado en java lo cual lo hace requerir de más recursos de hardware. Esto permitirá asumir el software de monitoreo Nagios siendo el mejor por ocupar menos recursos sobre un equipo el cual tiene las siguientes ventajas:

1. Software económico
2. Libertad de uso y redistribución
3. Independencia tecnológica

4. Soporte y compatibilidad a largo plazo
5. Sistemas sin puertas traseras y más seguros
6. Corrección más rápida y eficiente de fallos
7. Sistema en expansión.
8. Menor necesidad de técnicos especializados
9. Monitorización de equipos y redes
10. Gestión de procesos

2.9.1 Nagios detalla las actividades de monitoreo que realiza tales como:

1. Monitoreo de una máquina Windows.
2. Monitoreo de Switch y Reuters.
3. Monitoreo de equipos Linux/Unix.

2.9.2 Monitoreo equipos Windows.

En el monitoreo de una máquina Windows se debe tomar en cuenta las siguiente exigencias.

- Uso de memoria
- Carga del CPU
- Uso de disco duro
- Estado de servicios
- Ejecutar los procesos.

Se requiere de la instalación de un agente que actúa como plugin dentro del servidor de Nagios llamado check_nt, para comunicarse con el complemento NSClient++ de la máquina Windows realizando el monitoreo de la misma así como lo muestra el siguiente esquema.

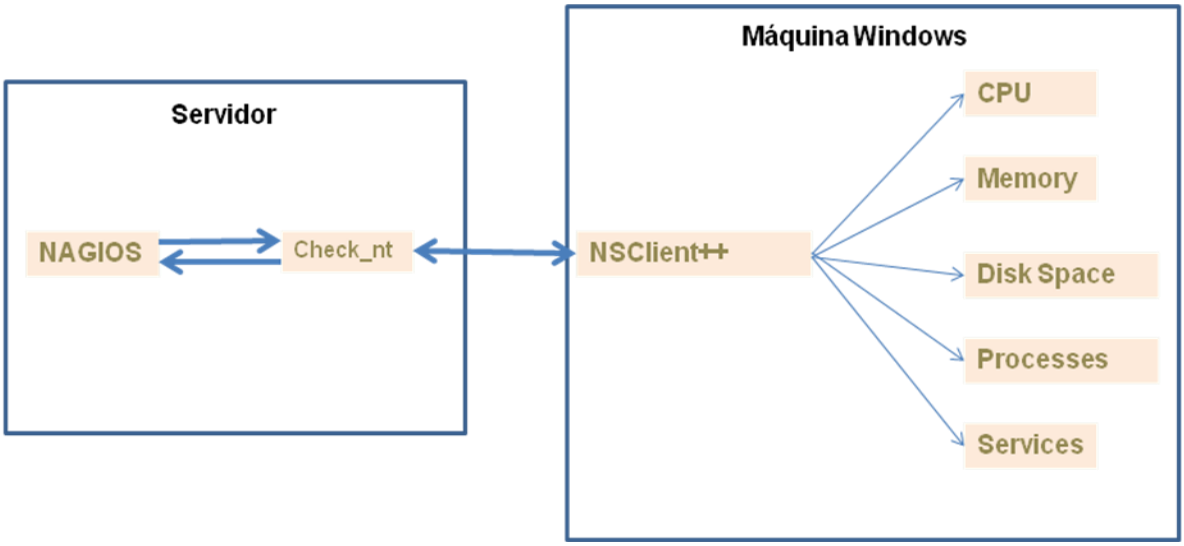


Imagen Nº 2.2 Monitoreo de máquina Windows

2.9.3 Monitoreo de equipos Linux/Unix

Al monitorear equipos Linux/Unix sedebe tomar en cuenta.

El uso el complemento NRPE, que permite ejecutar el plugin en equipos remotos Linux/Unix. Este complemento es útil si se necesita monitorear los recursos/atributos locales como uso en disco, carga en CPU, uso en memoria, para un equipo remoto.

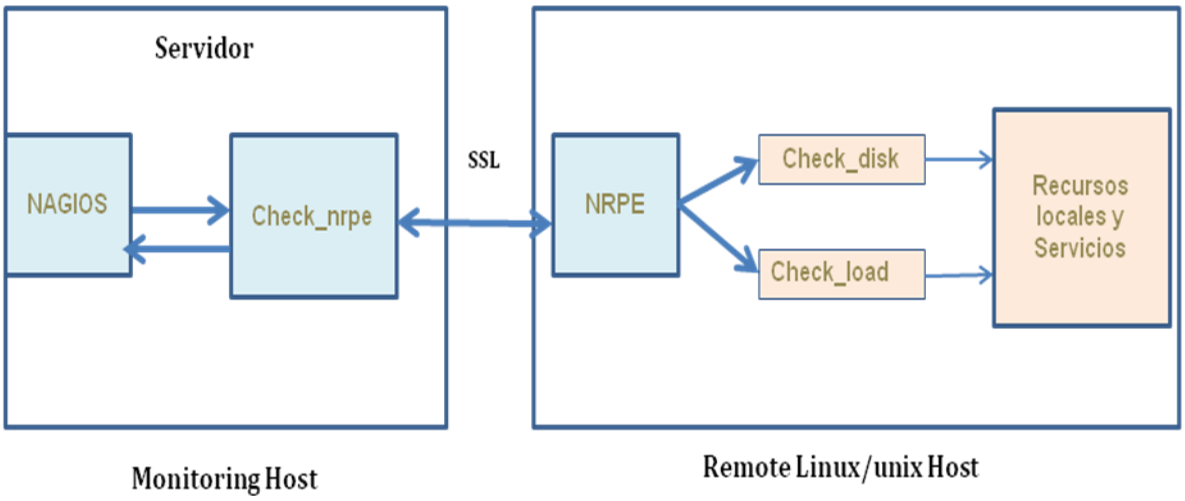


Imagen Nº 2.3 Monitoreo de máquina Linux/Unix

2.9.4 Monitoreo de Switch y Reuters

Los Switch y Routers pueden ser monitoreados fácilmente por Nagios para determinar pérdida de paquetes, Información sobre el estado usando SNMP y Ancho de Banda / Taza de Tráfico.

Para monitorear remotamente equipos Linux/Unix se debe usar el complemento NRPE que permite ejecutar el plugin en equipos remotos Linux/Unix. Este procedimiento puede ser útil si se necesita monitorear los recursos/atributos locales como uso en disco, carga en CPU, uso en memoria, etc. en un equipo remoto. Si el Switch soporta SNMP dentro de Nagios se monitorea el estado de los puertos, con el plugincheck_snmp.

El ancho de banda se monitorea utilizando MRTG con el plugincheck_mrtgtraf y recompila/reinstala los plugins de Nagios a si como se muestra en la siguiente figura.

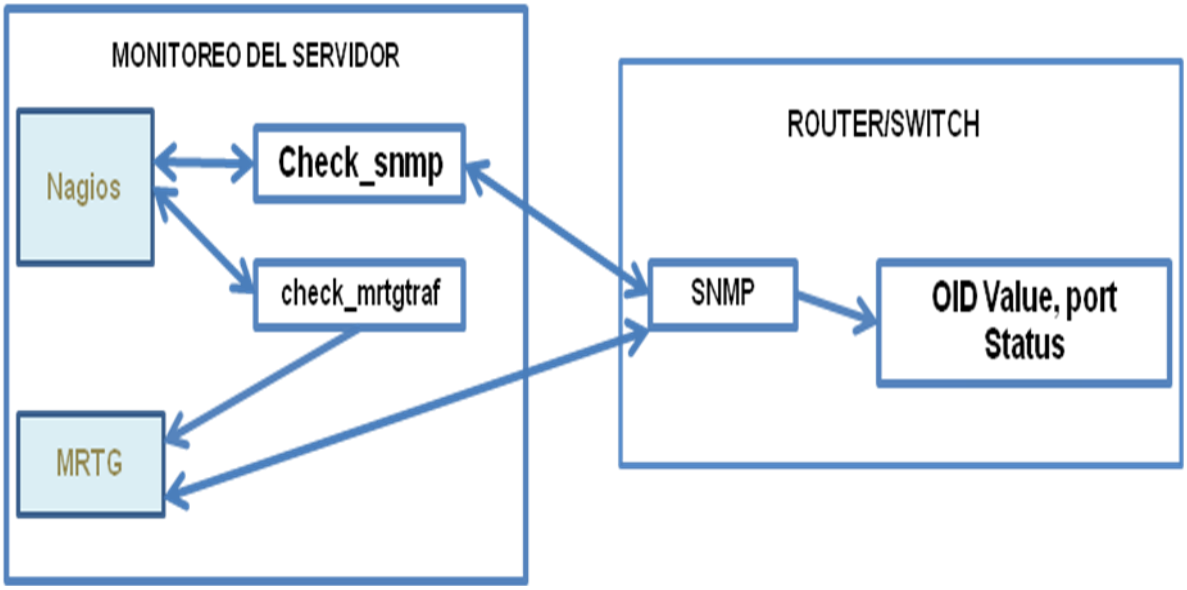


Imagen Nº 2.4 Monitoreo de los Switch y Reuters

2.10 Resumen del funcionamiento de la interfaz web Nagios

Nagios tiene servicios y máquinas y en la interfaz web el cual muestra distinta información sobre los equipos conectados a red. Además, cada vez que aparece un servicio o equipo en la web lo hace en forma de enlace por lo que, pinchando sobre el vínculo se conoce lo que hace ese servicio o máquina (según el caso).

Los pasos de la instalación Nagios para un mejor funcionamiento dentro de la conexión de red, es una herramienta económica para el MINSA y otras instituciones que deseen proteger sus quipos de cómputos conectados a red. Ver anexo # 6.pag:127.

A continuación mostraremos capturas de las partes más significativas de la interfaz y una pequeña explicación sobre cada una de ellas.

2.10. 1 Visión General

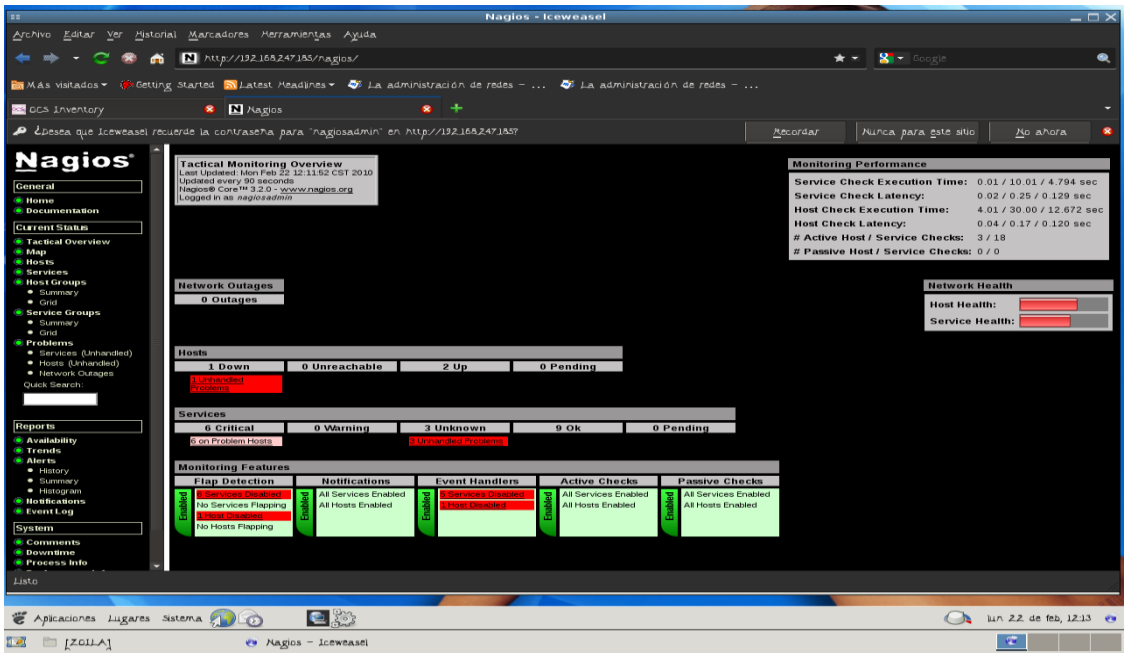


Imagen Nº 2.5 Detalles de equipos y servicios monitoreados por Nagios

Muestra de forma rápida un resumen de todo el sistema que permite tomar decisiones rápidas apoyadas en una base real de la interfaz.

2.10.2 Detalle de los servicios

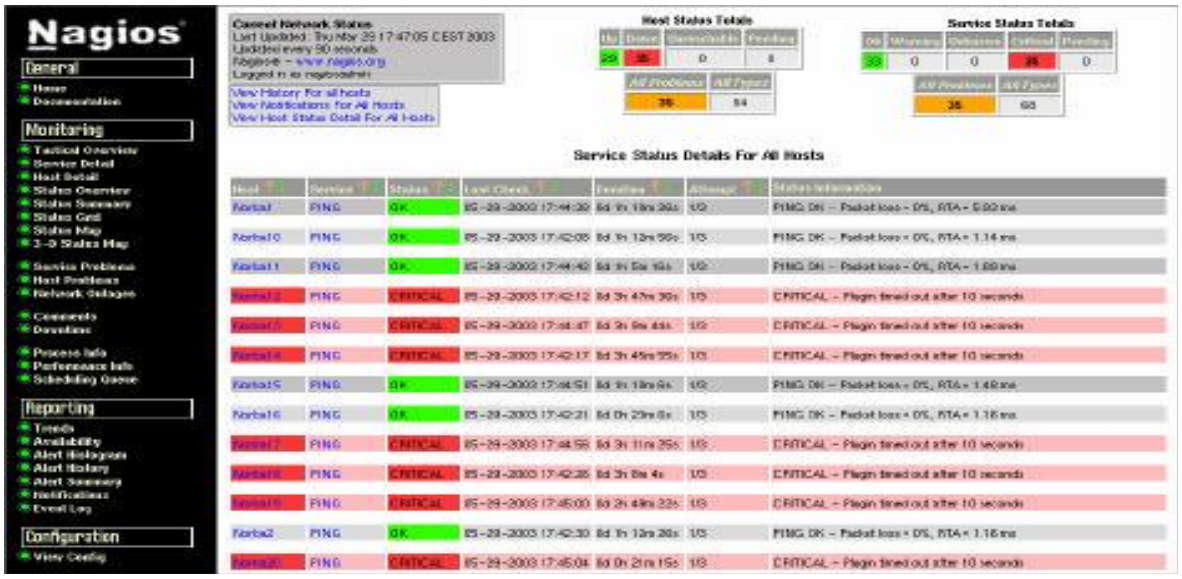


Imagen Nº 2.6 Detalles de los servicios monitoreados por Nagios

Muestra el estado de los servicios que se están monitoreando, así como una descripción textual de problemas de los equipos, Switch.

2. 10.3 Detalle de los equipos

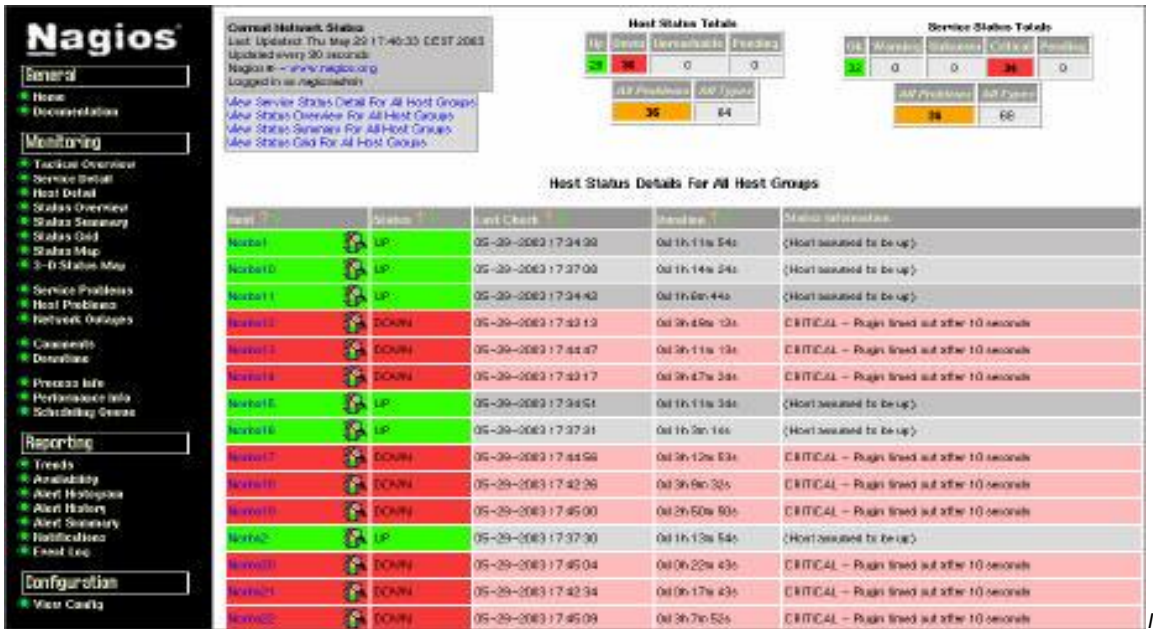


Imagen Nº 2.7 Detalle de los grupo de equipos monitoreados por Nagios

Muestran los equipos de cómputos activos, caídos y dañados que están siendo monitoreados por Nagios

2.10.4. Estado de un equipo

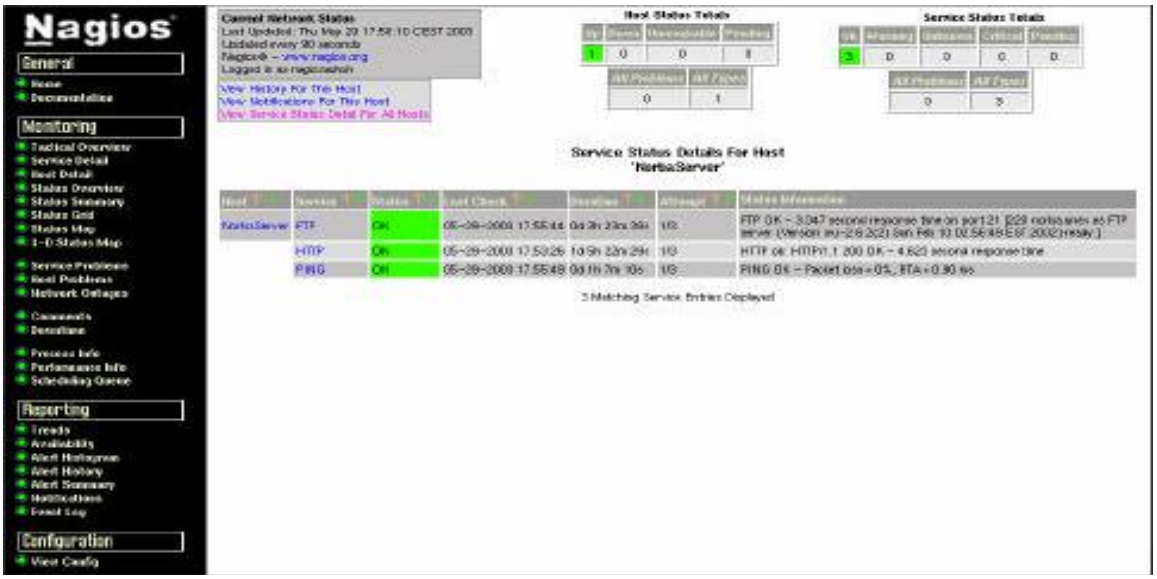


Imagen Nº 2.8 Detalle de los servicios por grupo monitoreados por Nagios

Muestra para cada equipo monitoreado, su estado, la fase de los servicios que tiene asociados y algunos datos extra.

2.10.5 Información sobre un equipo

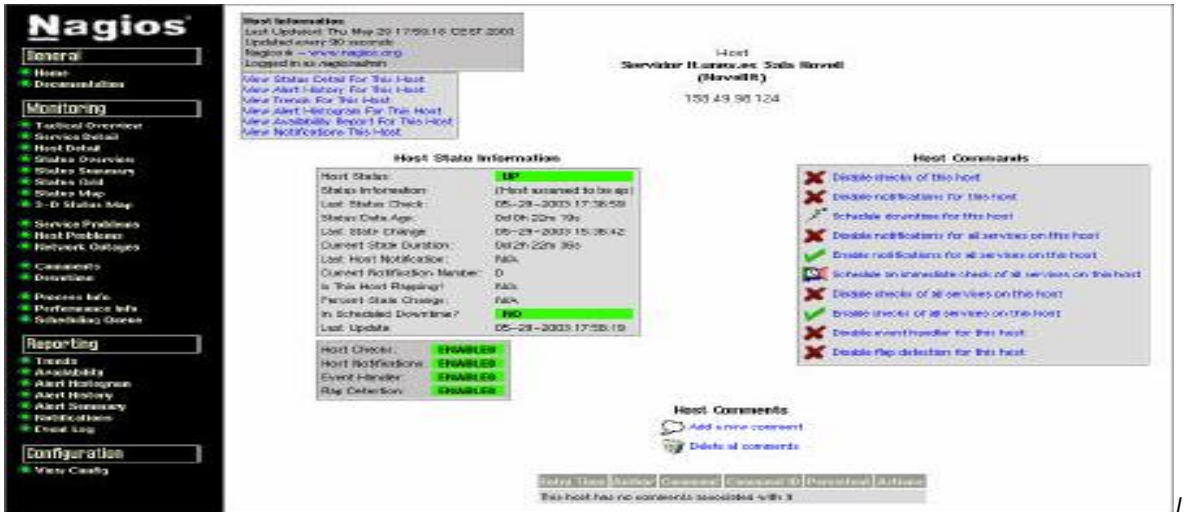
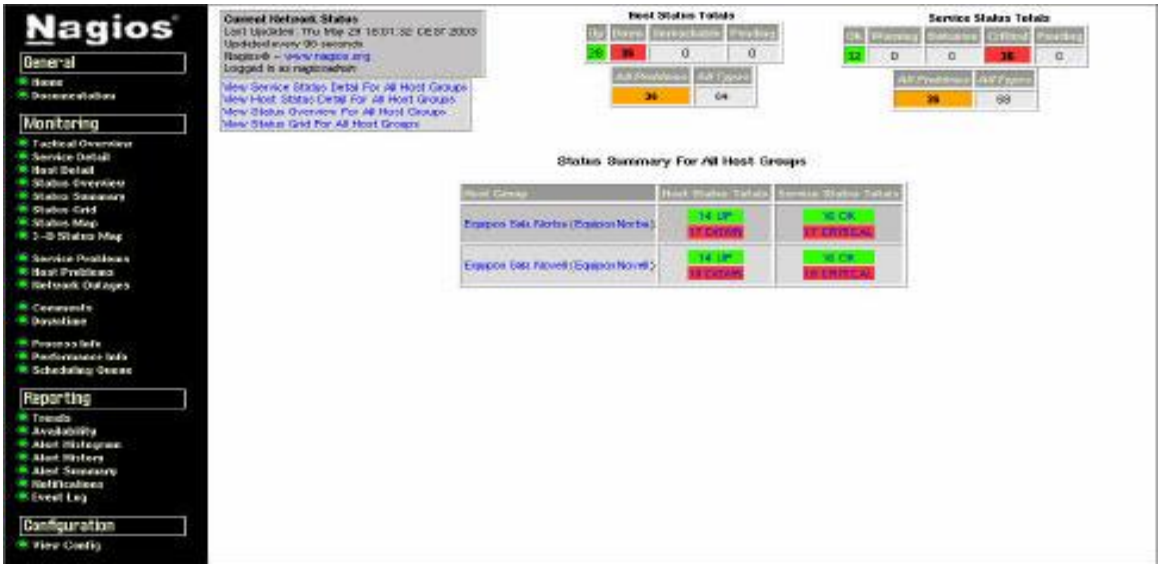


Imagen Nº 2.9 Detalle de los equipos

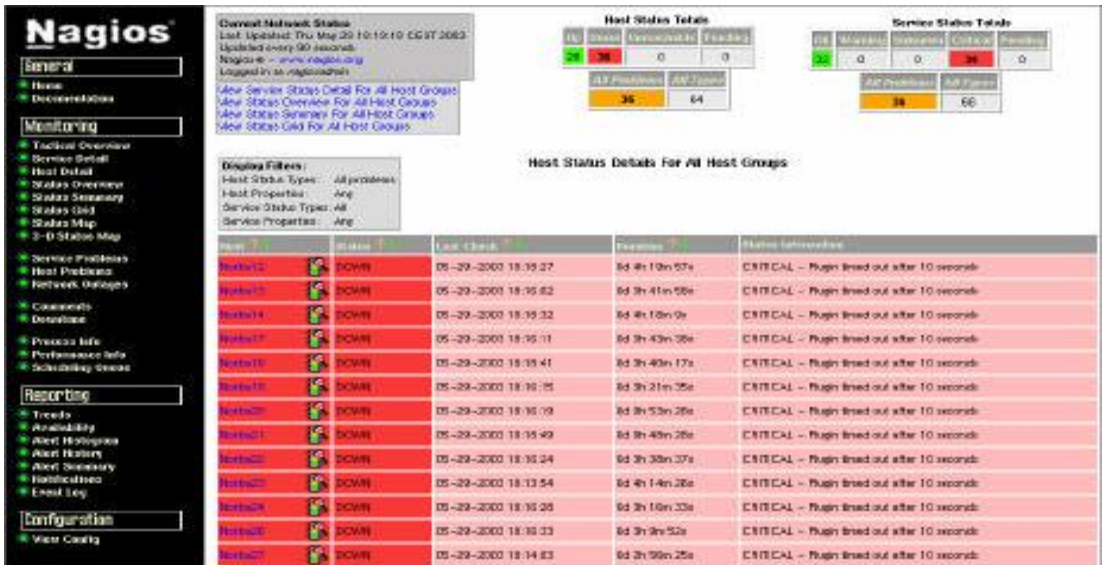
Muestra el detalle sobre un equipo concreto, permitiendo la ejecución de algunos comandos que afectan a dicho equipo.

2.10.6 Información sobre el estado de un equipo



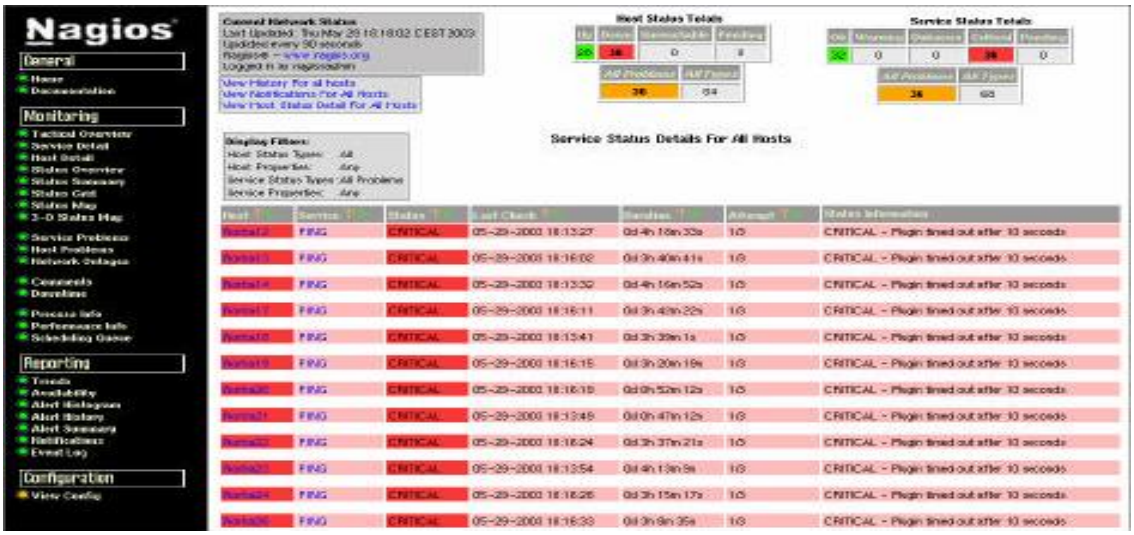
Muestra un resumen de los equipos y servicios activos y caídos según los grupos a los que pertenece cada grupo y de una forma amena, sencilla y muy rápida.

2.10.7 Problemas con los equipos



Esta opción muestra exclusivamente los equipos que están teniendo problemas así como una descripción de los mismos. Es especialmente útil para un administrador de red saber inmediatamente qué equipos están fallando.

2.10.8 Problemas con los servicios.



Esta opción muestra exclusivamente los servicios que están teniendo problemas así como una descripción de dichos problemas. Es especialmente útil para un administrador de red saber inmediatamente qué servicios están dejando de funcionar.

2.10.9 Creación de comentarios para equipos

Permite asociar un comentario a un equipo. Es especialmente útil si varios administradores por turnos administran las máquinas. Uno puede dejar notas sobre ciertos equipos para que otro las vea cuando llegue su jornada laboral.

2.11 Ventaja del software libre OCS-Inventory.

OCS- Inventory es una aplicación para el inventario de los PC's conectada a red, este procedimiento se realiza por medio de una estructura cliente servidor el cual se instala en el software agente de OCS-Inventory en cada uno de los pc's Windows y Linux, donde recopila toda la información de cada equipo de computo conectado a red, proyectando la información de cada dispositivo. Este software proporcionará al Ministerio de Salud las siguientes ventajas:

- Genera informes relevantes de inventario.
- Permite distribuir scripts sin sobrecargar la red.
- Cuenta con consola web de administración.
- Soporta sistemas Windows, Linux.
- Solo usa 5kb para empaquetar un inventario completo de Windows.
- Usa protocolos HTTP/HTTPS y formato de datos XML.
- Levanta inventario diario de un millón de computadores usando un servidor dual xeon de 3GHz con 4GB de RAM.
- El sistema operativo es apache, MySQL, PHP y PERL.
- Es accesible vía Web service a través de interfaz SOAP.
- El soporte de plug-insesa través de API.

El servidor de gestión OCS- Inventory contiene cuatros componentes principales los cuales son:

- Servidor de bases de datos es donde se almacena la información de los inventarios.
- Comunicación con el servidor este se encargas de comunicar el HTTP entre el servidor de bases de datos y el agente.
- Despliegue del servidor es donde se almacena todos los paquetes de configuración.
- La consola de administración es la que permite a los administradores consultar el servidor de bases de datos atreves de su navegador web favorito.

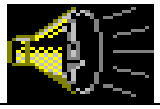
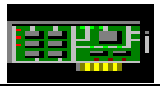
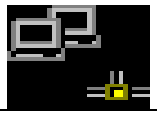
- El servidor de administración utiliza apache con MySQLserver y perl.
- El OCS es de multi-plataforma se ejecuta en el sistemas operativos Unix, a si como en Microsoft Windows 2000 o posterior a él.

Este software tiene una interfaz web privada escrita en PHP que ofrece servicios complementarios tales como:

- Consultar el inventarios
- Gestión de los derechos de los usuarios
- Una interfaz de los servicios de escritorio de ayuda para los técnicos.

Adicionalmente este software incluye la funcionalidad de distribución de paquetes instalación de aplicaciones, éstos son administrados a través del servidor y pueden ser instalados en cualquiera de los equipos conectados a red. La información que se muestra sobre el hardware y el sistema operativo de los ordenadores en red se refleja en el cuadro N° 2.3 del presente documento.

Se presenta los pasos de la instalación del OCS-Inventory en Debían para un mejor funcionamiento dentro de la conexión de red, siendo esta una herramienta económica para el MINSA y otras instituciones que deseen proteger sus quipos de cómputos. Ver anexo # 7. Pág.148.

Procesadores		Tipo (Pentium con MXX, Pentium II, Pentium III, Pentium IV, Celeron, Athlon, Duron), Velocidad de procesador, número de procesadores.
Dispositivos de entrada		Tipo (teclado o el señalar), fabricante, Descripción, descripción, interfaz utiliza (PS/2, USB).
Puerto del sistemas		Tipo (serial o paralelo), nombre y descripción
Reguladores de sistema		Fabricante, nombre, tipo (disco blando, IDE, SCSI, USB, PCMCIA, IEEE1394, infrarrojos).
Periférico de almacenaje		Fabricante, modelo, descripción, disco del tipo (flojos, duros, el CD-ROM, removible, graban), Tamaño en el MB.
Unidades lógicas/particiones		Unidad lógica, tipo (removible, duro, CD-ROM, red, RAM), Sistema de ficheros (FAT, FAT32, NTFS), Tamaño total en MB, espacio libre en el MB.
Dispositivos de sonidos		Fabricante, nombre, descripción
Adaptadores de videos		Nombre, chipset, memoria en MB, resolución de la pantalla
Adaptadores de la red		Descripción, tipo (terminal de marcado manual, Ethernet, token ring, atmósferas), La velocidad (en Mb/s o Gb/s), MAC address, IP address, mascara de la red del IP, entrada del IP, servidor del DHCP utiliza.
Impresoras		Nombre, controlador, puerto de la conexión.
Software		Extraído del registro según las indicaciones de agregue/quite el applet del panel de control del software: Nombre, editor, versión.
Sistema operativo		Nombre del SO y compañía registrada, dueño registrado, identificación registrada del sistema operativo del producto

Cuadro Nº 2.3 Información sobre hardware y sistema operativo inventariado por OCS Inventory

Capitulo 3. Documento tecnológico de normativas de seguridad informáticas

El propósito de las normas de seguridad es presentar los lineamientos de seguridad informática para la protección y garantía del buen funcionamiento de la infraestructura computacional y la seguridad a la información almacenada en los diversos equipos del Ministerio de Salud.

Visión .Construir un nivel de seguridad, altamente aceptable, mediante el empleo y correcto funcionamiento de las normativas de seguridad informática, basado en el sistema de gestión de seguridad de la información. Utilizando las técnicas y herramientas que contribuyan a optimizar la administración de los recursos informáticos del Ministerio de Salud.

Misión. Establecer las directrices necesarias en el correcto funcionamiento de un sistema de gestión para la seguridad de la información, enmarcado a un proceso de desarrollo continuo y actualizable y apegado a los estándares internacionales desarrollados para tal fin.

Este capítulo define las normativas de uso y seguridad que deben seguir todos los usuarios conectados a la red de datos del Ministerio de Salud. Han sido elaboradas con el objetivo de conseguir un uso más eficiente, correcto y seguro de los recursos informáticos.

Con estas normativas, el Ministerio de Salud logrará fomentar:

- La protección de las tecnologías de comunicaciones contra el acceso no autorizado desde adentro o fuera del MINSA.
- Que todos los usuarios del MINSA, tenga la responsabilidad de implementar estas normativas en sus respectivas áreas de trabajo.
- La integridad de los equipos de cómputo y la confidencialidad de la información contenida en ellos, será responsabilidad de División de Sistemas de Información.
- Los problemas relacionados con la seguridad informática deberán ser reportados al área de División de Información, para su debida solución.

El uso de los equipos de cómputos y de los medios de comunicación en los usuarios del MINSA, asumirán las siguientes responsabilidades:

- Tener conocimiento y comprensión correcta de todas las directrices e instrucciones contenidas en estas normativas de seguridad acerca del uso apropiado de los equipos.
- Hacer uso de las características de seguridad propia de los equipos, como las contraseñas.
- Asegurarse que cualquier información específica de un usuario individual como, cuentas de acceso y contraseñas, sean manejadas correctamente, no sean compartidas y hacer buen uso de ella.
- Reporte de cualquier incidente relacionado a la seguridad de los equipos y a la red, al personal de la División de Información.

Las responsabilidades de División de Sistemas de Información deberán:

- Asegurar que todos los responsables de áreas conozcan estas normas de seguridad informáticas y que los equipos de cómputos y la red de datos, no estén expuesta a amenaza proveniente del exterior.
- Velar por la seguridad de los activos informáticos.
- Publicar las normas de seguridad a nivel general.
- Dar cumplimientos a las normativas de seguridad informática.
- Elaborar un plan de seguridad informático.
- Informar sobre los problemas de seguridad a las autoridades del Ministerio de salud.

3.1. Normativas de uso de los recursos informático

1. El usuario es responsable del equipo de cómputo que se le asignó para su labor profesional.
2. Los equipos de cómputos del Ministerio de salud deben usarse en un ambiente seguro. Un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos.
3. Los usuarios tendrán acceso a los recursos de tecnologías respetando los lineamientos de seguridad del uso de recursos informáticos.
4. Las contraseñas tiene carácter confidencial e intransferible evitando su divulgación o préstamo.
5. Los servicios de correo debe utilizarse para fines de carácter laboral.
6. El software de comunicación a Internet será proporcionado y configurado a través de la División de Sistemas de Información.
7. Instalar en su equipo de cómputos los navegadores Mozilla Firefox e Internet Explorer.
8. El responsable de la unidad administrativa deberá realizar los trámites de recuperación en caso que se extravíe algún equipo o sufra daño por uso excesivo o mal uso por parte de los usuarios.
9. La división de sistema de información brindara los servicios técnicos de un equipo de cómputo.
10. Proteger los equipos de cómputos de la humedad excesiva.

3.2 Normativas para la instalación y administración de los recursos informáticos

El propósito de la norma es garantizar un nivel de seguridad adecuado a los equipos y recursos informáticos del Ministerio de Salud.

1. Proteger los equipos e instalaciones del Ministerio de Salud de un indicio de violación a la seguridad de la información.
2. Tener actualizado un control de las claves de usuarios y contraseñas utilizadas en los servidores y equipos críticos.
3. Realizar configuraciones necesarias para garantizar la disponibilidad de la información almacenada en las bases de datos.
4. Los usuario no podrán realizar copias de los software, código fuentes u objetos de las aplicaciones o sistemas.
5. Evadir programas de mensajería y conversación local y vía Internet. (CHAT'S).
6. Instalar programas con licencia a los equipos informáticos propiedad del Ministerio de Salud.
7. Se realizará monitoreo a la red de datos en función de controlar el tráfico que circula por el nodo.
8. Utilizar correctamente los recursos informaticos, servicios de navegación por internet y correo.
9. El respaldo de la informacion debera hacerse en hora de menos carga del sistemas.
10. Aplicar actualizaciones de seguridad para el sistema operativos que se este usando.
11. Instalar en su equipos de computo sólo el software que sea necesario

3.3. Normativas para el uso de servidores

1. Los servidores, equipos de telecomunicaciones y demás equipos críticos deben contar con claves de acceso y contraseñas.
2. El personal autorizado administrativo tendrá el acceso a la contraseña de los servidores.
3. Las claves de acceso de los servidores de correo, internet, aplicaciones y respaldo son de uso exclusivo de los administradores de la red.
4. Las contraseñas que se le asigne a cada servidor deberán tener 16 caracteres como mínimo combinado letra mayúscula, minúscula o número simbologías.
5. El acceso a los servidores Windows o Linux/Unix de manera remota se realizará por medio de un login o un pasword, a través de un servicio seguro como el ssl como transferencia de archivos
6. Toda la información de los servidores de bases de datos y de respaldo debe tener un control de seguridad para garantizar que no sea copiada ni robada.

3.4 Normativas de respaldo de servidores.

1. El administrador de la red será el responsable de realizar y verificar los respaldos de los servidores cada dos días.
2. El respaldo del sistema operativo, programas del sistema y su configuración deberán realizarse en base a la característica del equipo.
3. El área de informática deberá cumplir con una bitácora para el registro y control de los respaldo de los servidores, lo cual tendrá los siguientes datos, fecha y contenido del respaldo, nombre y firma de la persona que lo realizó y del supervisor.
4. El administrador de servidores debe realizar revisiones sin previo aviso de las bitácoras de los respaldo.

5. Realizar un respaldo con anticipación antes de efectuar el mantenimiento preventivo o correctivo a los servidores de la red.
6. El acceso de la configuración de los sistemas operativos de los servidores, es únicamente permitido al administrador de la red.

3.5 Normativas de operación de la División de Sistemas de Información

1. Restringir la entrada al centro de cómputo a persona ajena a la institución, solo podrá acceder con una solicitud por escrito y previa autorización del responsable de informática.
2. Presentar un permiso firmado por el responsable de informática para realizar el movimiento de un equipo de cómputo fuera de la institución.
3. El centro de cómputo debe de operar a una temperatura de 19º c, además tener dispositivo contra incendios especiales para equipo de cómputos.
4. El usuario debe evitar fumar, comer y beber dentro de las instalaciones del centro de cómputo.
5. Depositar la basura en su lugar y mantener su lugar de trabajo ordenado.
6. Se sancionará al usuario que sea sorprendido alterando configuraciones de software en los equipos de cómputo.
7. En caso de incumplimiento a los presentes lineamientos, la dirección superior del MINSA e Informática podrá tomar acciones o medidas para su cumplimiento, llegando hasta la cancelación del servicio.
8. La División de Sistemas de Información, divulgará las normativas y estándares de seguridad informática. Efectuara el seguimiento y cumplimiento de los lineamientos informáticos, reportándolos a la Dirección General en caso de incumplimientos.

3.6 Normativas de mantenimiento preventivo y correctivo de los equipos informáticos

1. Al realizar los mantenimientos preventivos y correctivos a los equipos de cómputos, se debe avisar su realización con anticipación en un periodo de 3 días hábiles antes de la fecha programada.
2. Se dará atención a la reparación del equipo y servicio informático, solamente al que sea reportado en los formatos establecidos por el área de informática.
3. El responsable de informática tiene la obligación de vigilar el procedimiento del mantenimiento preventivo y correctivo que el personal técnico lleva acabo.
4. Llevar un control de los mantenimientos de soporte técnicos que se realizan a diario en la institución.
5. Los equipos de propiedad personal, quedan excluidos de todo programa de mantenimiento preventivo y/o correctivo dentro del Ministerio de Salud.

6. Solo el personal de informática debe realizar reparaciones al equipo de cómputos.

7. El área de informática será responsable de planificar los mantenimiento preventivo de los equipo de cómputo del ministerio de Salud.

8. Se llevara un control del equipo en garantía o tenga exclusividad de patentes.

9. Se reportaran las fallas que presente el cableado estructurado o en los servicios datos.

10. El servicio de mantenimiento de sistemas, será prestado a aquellos que se encuentren registrados en la subdirección de Informática y de los cuales se cuente con la documentación respectiva, así como de los programas desarrollados para su implantación.

3.7 Normativas de acceso remoto

1. Los usuarios conectados a la red LAN a través de cualquier tipo de acceso remoto deberán respetar las normas de seguridad de acceso remoto.
2. El usuario con conexión no autorizada será desconectado de la red LAN.
3. La División de información es responsable de proporcionar el servicio de acceso remoto y las normas de acceso a los recursos informáticos disponibles.
4. El usuario de estos servicios deberá sujetarse al reglamento de uso de la Red del Ministerio de Salud, en concordancia con los lineamientos generales de uso de Internet.
5. El acceso remoto que realicen personas ajenas a la institución deberá cumplir las normas que emite el Ministerio de Salud.

3.8 Normativas de uso de correo electrónico

1. Todos los usuarios con una cuenta válida podrán enviar y recibir correo electrónico dentro y fuera del MINSA siempre y cuando hayan sido autorizados por la dirección.
2. Los buzones de correo deben ser respaldados regularmente.
3. Toda comunicación a través del correo electrónico dentro y fuera del MINSA será revisada para garantizar que no contengan virus o cualquier otra forma de código malicioso.
4. El correo electrónico no debe utilizarse como herramienta de difusión de información masiva.
5. Las cuentas creadas en los servidores de la red de Ministerio de Salud tienen como objetivo el intercambio de mensajes propios al desempeño profesional.
6. Se niega el uso de cuentas de correo distintas a las proporcionadas por la División de Sistemas de Información.

7. Ningún empleado autorizado a usar Internet o correo electrónico podrá reclamar interés propietario de los servicios.
8. Borrar cada quince (15) días la correspondencia electrónica archivada de manera que se pueda utilizar al máximo el espacio en el disco de la computadora.
9. Los mensajes de correo que tienen más de tres meses en el buzón serán eliminados por el administrador de la red.
10. Es necesario que los usuarios con cuenta de correo deberá vaciar la bandeja de entrada y salida para evitar saturar el servidor de correos.
11. Se realizará un monitoreo periódico sobre el uso de los correos, a fin de dar de baja aquellas cuentas que no sean utilizadas.

3.9 Normativas de seguridad física

1. Las oficinas técnicas y administrativas direcciones y divisiones deben contar con sistema de vigilancia las 24 horas del día, de lunes a domingo.
2. El acceso del personal, visitas a las instalaciones administrativas y/o técnicas de la compañía del MINSA, debe ser controlado y debidamente registrado.
3. El ingreso del visitante debe ser autorizado por el trabajador que recibe la visita, comunicándolo al personal encargado de coordinar el ingreso a la institución.
4. Presentar su cedula de identidad al ingresar a las instalaciones del Ministerio de salud.
5. Se le asigna un carnet de identificación de VISITANTE al personal ajena a la institución.
6. Los usuarios externos a la institución deberán respetar las áreas restringidas.
7. Las oficinas deben tener una temperatura ambiente a 20° centígrados.

3.10 Normativas de uso de software antivirus

1. La División de Información proveerá los medios para descargar e instalar las versiones actualizadas del software antivirus.
2. Asegurar que el equipo conectado a red ejecute la versión actualizada del software antivirus en todo momento.
3. Instalar y activar la herramienta de software antivirus con licencias vigente.
4. Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y llamar a informática.
5. Para restaurar los programas infectados por virus, deben hacerse copias de todo software antes de su uso y deben guardarse en un lugar seguro.
6. El uso de medios de almacenamiento en cualquier computadora de la institución deben estar libres de virus u otros agentes dañinos.
7. El escáner del software antivirus trabajara en todos los equipos de cómputos conectado a red en horas de almuerzo.
8. Cada usuario que tenga bajo su resguardo algún equipo de cómputo personal o portátil, será responsable de solicitar a informática la actualización del software antivirus.
9. Instalar herramientas de seguridad automatizados que sirven para proteger o salvaguardar a la infraestructura tecnológica.
10. El Software antivirus realizara el scanner automáticamente sobre los activos conectados a red en horas del almuerzo.

3.11 Normativas del control de acceso a los sistemas

1. Implantar un sistema de autorización y control de acceso con el fin de restringir las lecturas, escrituras, modificar, crear, o borrar datos importantes.
2. Los usuarios no realizaran conexión por módems en las PCs, para prevenir la incursión de intrusos informáticos a través de puertas traseras.
3. Los usuarios no podrán extraer datos fuera de la sede de la institución sin la aprobación previa.

3.12 Normativas de seguridad de la información

1. Periódicamente se debe realizar el respaldo de los datos guardados en PCs y servidores y guardarse en un lugar seguro, a prueba de hurto.
2. El equipo de informática es responsables de proteger los programas y datos contra pérdida o daño.
3. La información del Ministerio de Salud es confidencial y uso restringido, por tanto debe guardarse y transmitirse en forma cifrada, utilizando herramientas de encriptado robustas y que hayan sido aprobadas por el área de Informática.
4. La información deberá estar protegida en medio físico como documento escrito, disco compacto debe ser resguardada bajo llave.
5. Todos los sistemas conectados a Internet debe tener un proveedor compatible versión del sistema operativo instalado.
6. Los sistemas conectados a internet debe estar al día con los parches de seguridad.
7. Revisión constante de los sistemas eléctricos.

3. 13 Normativas de ética al administrador de los servidores de red

1. El administrador no tendrá acceso a las lectura de correos electrónico de los usuarios.
2. Supervisar el cumplimiento de los lineamientos de seguridad informáticas institucionales.
3. El acceder a la información de otro trabajador, sin la presencia de él, o sin previa autorización del jefe inmediato superior.
4. Operar los servidores de acceso a cada uno de los servicios que se brinde quedando limitado exclusivamente a los usuarios.
5. Velar por los aspectos de la seguridad informática, garantizando que los servidores estén configurados y operados en forma correcta.
6. Reportar la anomalía que se detecte en el funcionamiento de los servidores, informarlo inmediatamente al nivel superior y reflejarlo en el libro de incidencias.
7. El administrador está en la obligación de garantizar que la información que se genere o se reciba cumpla con lo regulado por la dirección del Minsa Central.
8. Utilizar el servidor de correo para monitorear el desempeño de los empleados.
9. Faltar al compromiso de la ética profesional realizando acciones como: husmear conversaciones en línea para uso destructivo en contra del usuario.
10. Llevar un registro y control de las direcciones IP de los equipos conectados a la red con acceso a Internet y la información de los usuarios, así como notificar al Departamento de Redes y Comunicaciones de las altas y bajas de usuarios para los servicios de correo electrónico e Internet.

3.14 Normativas de seguridad lógica

1. Restringir el acceso a los programas y archivos que son propiedad del Ministerio de Salud.
2. Supervisar a los usuarios de no modificar los programas ni archivos que son propiedad de la institución.
3. Utilizar datos, archivo y programas correctos con procedimiento adecuados.
4. Asegurarse que la información recibida por el destinataria sea la misma que ha sido trasmitida.
5. Utilizar herramientas adecuadas para la administración de la red.

3.15 Normativas de seguridad de red inalámbrica

1. Activar la herramienta del firewall para proteger la red inalámbrica.
2. La división de sistemas de información deberá proteger los puntos de acceso inalámbrico.
3. Los puntos de acceso inalámbrico deberán utilizar alguna forma de autenticación de usuarios, antes de dar acceso a la red cableada.
4. Los dispositivos de usuario deberán soportar autenticación para acceder a la red inalámbrica.
5. Proteger la seguridad de los puntos de acceso Inalámbrico y otros componentes de la red inalámbrica.
6. Los datos transmitidos por la red inalámbrica deberán ser encriptados por el área de informática.
7. Habilite el control de acceso por direcciones MAC. Como una barrera para un supuesto atacante.
8. Deshabilite servicios innecesarios en su router, como el SNMP, Telnet, SSH para evitar conexiones ilegales.

9. Deshabilitar el acceso de internet vía inalámbrica de tal manera que pueda ser accesible solo por cable.
10. Desactive la opción de SSID para que la red no sea visible en el aire y realicen una conexión ilegal.
11. Desactive la opción de DHCP, entregue direcciones IP estático a la red LAN.
12. El rango de direcciones IP LAN de muchos equipos es: 192.168.x.x. cámbienlo por un número menos adivinable, por ejemplo 90.0.0.0 /24.
13. Usar VPN con cifrado para conectarse a la red Wi-Fi.
14. Cambie regularmente sus claves de conexión WI-Fi para evitar malversación.

3.16 Normativas de seguridad de prevención de intrusos maliciosos

1. Los servidores y equipos de telecomunicaciones expuestos a internet deberán de tener abiertos los puertos necesarios para las aplicaciones.
2. Todos los equipos bajo la plataforma Windows y Linux deberán de contar con todas las actualizaciones pertinentes.
3. Todos los equipos informáticos deberán contar con la última actualización de antivirus y verificar el tipo de ataque que está presentado. ya sea interno o externo y tomar las acciones necesarias en los equipos locales y/o servidores expuestos a Internet.
4. Realizar monitoreo del equipo designado para prevención de intrusos.
5. Todos los equipos informáticos deberán de contar con la última actualización de anti spam.

3.17 Normativas de acceso a las aplicaciones

1. Las aplicaciones deberán estar correctamente diseñadas, en funciones de acceso para cada usuario.
2. Se deberán definir los permisos sobre las aplicaciones y archivos.
3. Llevar un registro de las aplicaciones, sobre las actividades de los usuarios en cuanto al acceso, errores de conexión, horas de conexión entre otros.
4. Asegurar la última versión del firmware del router; para evitar la incorporación de virus en los agujeros de seguridad.

3.18 Normativas de seguridad organizacional

1. El usuario acatará las disposiciones expresas sobre la utilización de los servicios informáticos y la red institucional.
2. El administrador hará respaldo periódicos de la información así como la depuración de los discos duros.
3. El administrador revisará el tráfico de paquetes que se estén generando dentro de un segmento de red, a fin de determinar si están haciendo mal uso de la conexión del punto.
4. El administrador monitoreara las acciones y tareas de los usuarios de la red institucional.
5. El usuario tienes derecho a los servicios de internet mediante la aceptación de las normativas de seguridad informática.
6. La institución deberá ser de conocimiento al personal de las normativas de seguridad informática vía correo electrónico, capacitación al personal, colocación el lugares visible y distribución impresa.
7. Respetar y cumplir las normativas en función de las tecnologías de comunicaciones.

3.19 Normativas de control de acceso a la red

1. El administrador de sistemas diseñará los mecanismos necesarios para proveer acceso a los servicios de la red institucional.
2. Los mecanismos de autenticación y permisos de acceso a la red, deberán ser evaluados y aprobados por el gestor de seguridad.
3. El comité de seguridad, hará evaluaciones periódicas a los sistemas de red, con el objetivo de eliminar cuentas de acceso sin protección de seguridad, componentes de red comprometidos.
4. El administrador de sistemas, verificará que el tráfico de red sea, estrictamente normal.
5. Los dispositivos de red, estarán siempre activos, y configurados correctamente para evitar anomalías en el tráfico y seguridad de información de la red institucional.
6. Se utilizarán mecanismos y protocolos de autenticación como: IP, claves públicas y privadas, autenticación usuario/contraseña.
7. Los puntos de acceso inalámbrico deberán utilizar alguna forma de autenticación de usuarios antes de dar acceso a la red cableada.
8. Los dispositivos de usuario deberán soportar autenticación para acceder a la red inalámbrica.

3.20. Normativas de monitoreo del acceso y uso del sistema Nagios

1. Los administradores de red tendrán especial cuidado al momento de instalar las aplicaciones de Nagios en los servidores.
2. Configurar correctamente cada servicio del software libre con sus respectivos permisos de ejecución.
3. Realizar las actividades de configuración de los sistemas de red.
4. Las aplicaciones de los servicios correrán con cuentas restringidas y con privilegios de la cuenta administrativa.

5. El servidor de dominios, verificará y desactivará cualquier estación de trabajo, que este en uso después de la hora de salida o finalización de la jornada laboral.
6. Los servidores estarán debidamente configurados, evitando el abuso de personal extraño a la administración.
7. Efectuar configuración de los servicios y acceso exclusivo mediante una cuenta referida al servicio.
8. La cuenta administrativa, es propiedad exclusiva del administrador de sistemas.

3.21 Normativas del cumplimiento técnico de la revisión y actualización de las políticas de seguridad informáticas.

1. La documentación de seguridad será actualizada respetando todas las normativas que demandan su correcto diseño y aplicabilidad.
2. Los responsables de la actualización y aprobación de las normativas de seguridad, deberán ser designados como propietarios de los cargos de actualización y aprobación de los mismos.
3. El personal o usuarios de la red institucional deberán tener pleno conocimiento de la documentación de seguridad, apegarse a ella en todo caso o gestión.
4. El medio exclusivo de soporte para la seguridad de la información, lo constituyen las políticas de seguridad informática y toda su reglamentación técnica, esto incluye un sistema de gestión de seguridad de la información.
5. Se suspenderá por un año, el incumplimiento de la normativa de seguridad informática o de protección de datos.
6. Se aplicara sanciones por violación a la seguridad informática de la institución.

3.22 Plan de contingencias informáticas

Se propone a la división de sistemas de información crear para cada aéreas de trabajo del Ministerio de Salud un plan de contingencias informáticas que incluya los siguientes puntos:

1. Continuar con la operación del área con procedimientos informáticos alternos.
2. Tener los respaldos de información en un lugar seguro.
3. Tener el apoyo por medios de dispositivos o en forma documental, de las operaciones necesarias para reconstruir los archivos dañados.
4. Contar con un instructivo de operación para la detección de posibles fallas, para que toda acción correctiva se efectúe con la mínima degradación posible de los datos.
5. Contar con un directorio del personal interno y del personal externo de soporte, al cual se pueda recurrir en el momento en que se detecte cualquier anomalía.
6. Ejecutar pruebas de la funcionalidad a la tecnologías informáticas
7. Mantener revisiones del plan a fin de efectuar las actualizaciones respectivas.

VII. CONCLUSIONES

En el estudio del diagnostico se propone la alternativa de la herramienta del software de monitoreo Nagios y OCS Inventory en solución al problema que genera los sistemas de red sobre los equipos informáticos y la información contenidas en ellas.

Se propone desagregar la división de sistemas de información y reorganizar las funciones profesionales facilitando así, una repuesta más eficaz a nivel laboral y tecnológico, donde se proponen fichas ocupacionales a los puestos de: Administración de Información, Asistente, Soporte Técnico y Analista de Sistemas para ser agregados al manual de funciones.

Hubo una evaluación de riesgo a escala cualitativa y cuantitativa para medir el grado de afectación que inciden en los activos informáticos, logrando mitigar los peligros de mayor incidencia.

Se proponen normativas de seguridad informáticas para garantizar una protección adecuada y mejorar los problemas que generan los sistemas de red bajo la normativa ISO/IEC 27001.

VIII. RECOMENDACIONES

Recomendamos

1. Que el MINSA se certifique bajo el estándar ISO/ICE 27001 para incorporar sus tecnologías bajo un Sistema de Gestión de la Seguridad de la Información (SGSI).

2. Un plan de acción para la utilización del manual de normativas de seguridad informática.

3. Realizar una evaluación de riesgos anualmente para medir el grado de incidencias sobre los peligros informáticos.

4. Aprobar y poner en marcha el manual de normativas de seguridad informática.

5. Utilización del software libre Nagios y el OCS-Inventory como una herramienta de seguridad informática para monitorear los equipos y servicios conectados a red, permitiendo controlar los riesgo que circulan por el trafico del punto de conexión.

6. Capacitación del personal de la División de Sistemas de Información, en el uso de las normativas ISO/ICE 27001

7. Capacitar al personal en general sobre el estándar NFPA (National Fire Protection Association) 10, 3-1.2.4: "Edificios que estén expuestos a fuegos de clase C, deberán incluir extintores de clase A para la protección general del edificios. Los extintores de clase C para la protección de equipos eléctricos.

IX. GLOSARIO

1. **Análisis de riesgos** Es un entorno informático donde existen una serie de recursos humanos, técnicos y de infraestructura entre otros que están expuestos a diferentes tipos de riesgos.

2. **Activos** Recursos del sistema de información necesarios para de una Organización

3. **Amenaza** Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

4. **Análisis de Riesgos** Proceso sistemático para estimar la magnitud de los peligros a que está expuesta una Organización.

5. **Ataque** Cualquier acción deliberada encaminada a violar los mecanismos de seguridad de un sistema de información.

6. **Confidencialidad** Proteger la información de su revelación no autorizada.

7. **Disponibilidad** Los recursos de información sean accesibles, cuando estos sean necesitados.

8. **Estándares** Son acuerdos documentados que contienen especificaciones técnicas u otros criterios precisos para ser usados como reglas, guías para asegurar que los materiales, productos, procesos, productos y servicios cumplan con su propósitos.

9. **Impacto** Consecuencia que sobre un activo tiene la materialización de una

10. **Integridad** Proteger la información de alteraciones no autorizadas por la organización.

11. **Normas** Son reglas predeterminadas, estándares o medidas con la que podemos valorar un acto.

12. **Riesgos** Estimación del grado de manifestación a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

13. **Seguridad en redes** Es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado.

14. **Seguridad informática** Consisten en asegurar que los recursos del sistema de información de una organización sean utilizados correctamente.

15. **Organización** se refieres a la estructura técnica de las relaciones, que deben darse entre las jerarquías, funciones y obligaciones individuales necesarias en un organismo social para su mayor eficiencia.

16. **Soporte Técnico: (Personal en Outsourcing)** Personal designado o encargado de velar por el correcto funcionamiento de las estaciones de trabajo, servidores, o equipo de oficina dentro de la institución.

17. **Normativa de Seguridad ISO/IEC 17799:** (Código de buenas prácticas, para el manejo de seguridad de la información) Estándar o norma internacional que vela por que se cumplan los requisitos mínimos de seguridad, que propicien un nivel de seguridad aceptable y acorde a los objetivos institucionales desarrollando buenas prácticas para la gestión de la seguridad informática.

18. **Normativas de seguridad ISO/IEC 27001:** Establece los requisitos para un Sistema de Gestión de la Seguridad de la Información (SGSI) y complementa con el estándar ISO/CEI 17799, código de buenas prácticas, asegurando la selección de controles de seguridad adecuados que protejan los activos de información y ofrezcan confianza a todas las partes interesadas.

19. **COBIT** Es el marco aceptado internacionalmente como una buena práctica para el control de la información, TI y los riesgos que conllevan. Se utiliza para implementar el gobierno de IT y mejorar los controles de IT. Contiene objetivos de control, directivas de aseguramiento, medidas de desempeño y resultados, factores críticos de éxito y modelos de madurez.

20. **Estándar TIA/EIA 568B1**Esta norma describe el diseño y construcción de rutas y espacios de telecomunicaciones dentro y entre edificio comerciales.
21. **ISO 27001** ISO internacional ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los Responsables de iniciar, implantar o mantener la seguridad de una Organización.
22. **ITIL** Brinda una descripción detallada de un número de prácticas importantes en IT (tecnología de información), a través de una amplia lista de verificación, tareas, procedimientos y responsabilidades que pueden adaptarse a cualquier organización.
23. **ISO** (Organización Internacional de Estándares) Institución mundialmente reconocida y acreditada para normar en temas de estándares en una diversidad de áreas, aceptadas y legalmente reconocidas.
24. **IEC** (Comisión Electrotécnica Internacional) Junto a la ISO, desarrolla estándares que son aceptados a nivel internacional.

XI. BIBLIOGRAFIA

Textos

1. Hernández Sampieri Roberto, Metodología de la investigación, segunda edición. Eco Umberto, Proyecto de investigación, primera edición.
2. González Báez Julissa, Tesis Implementación de un sistemas de información las instalaciones del área de insumos médicos del MINSA el hospital regional de Asunción Juigalpa – Chontales durante el periodo 2002- 2003.
3. Guevara Campos Ana Carolina, Cruz Gómez Wendy María, Tesis Auditoria informática Aplicada en la Procuraduría de la República de Diciembre del 2005 a Septiembre del 2006.

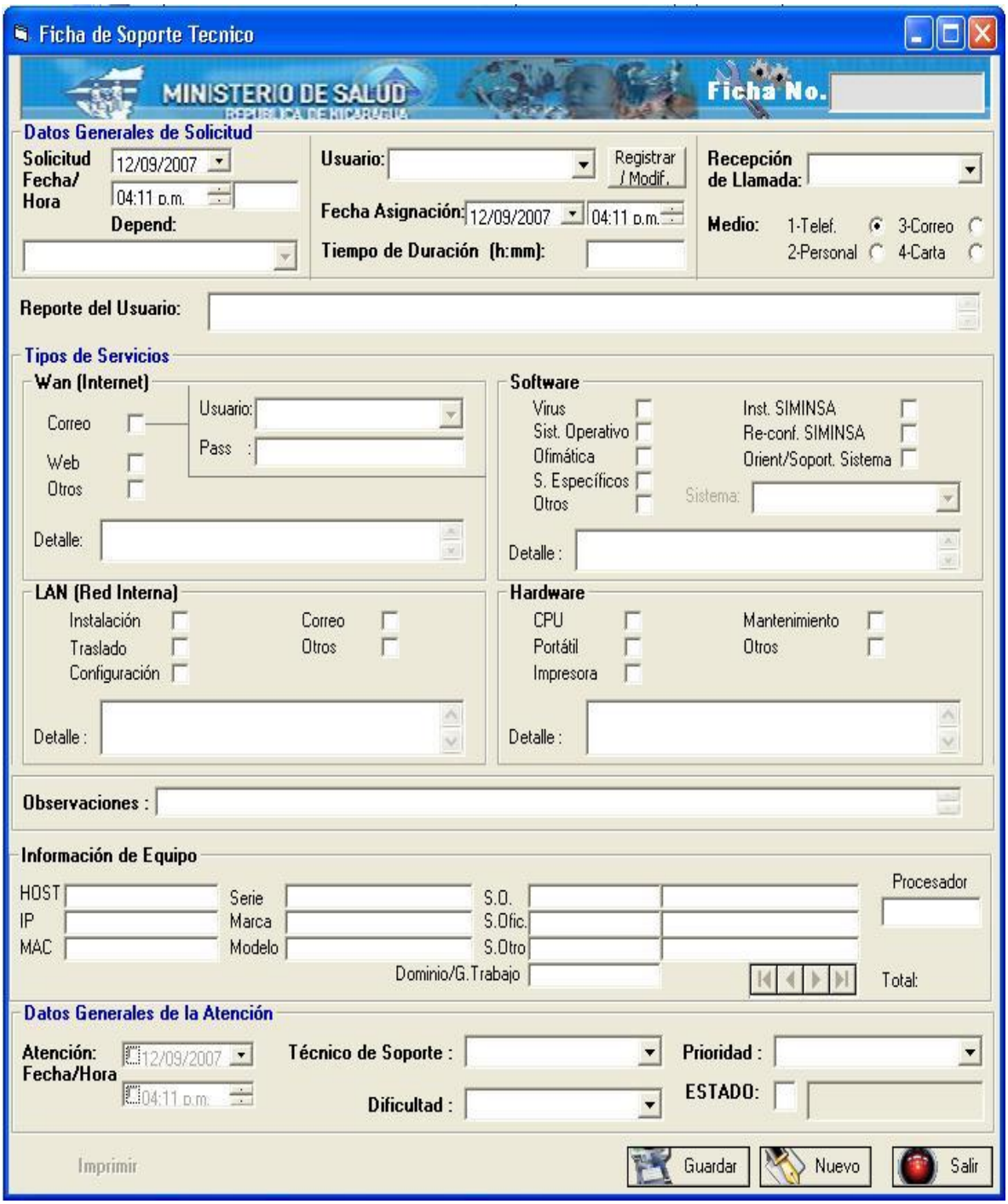
Recursos de Internet

1. www.csi.map.es, 2009
2. www.bvindecopi.gob.pe/normas/isoiec17799., 2008
3. www.bvindecopi.gob.pe, 2008
4. ISO 27000, 2008
5. Analisis comparativo de la normas iso 27000 y la norma iso 17799, 2009
6. Getion de riesgos, 2009
7. Mecanismo de seguridad de redes Estándares tecnológicos institucionaleswww.enterate.unam.mx,www.rediris.es/ , 2007
8. Normas ISO 9000: su Base , 2009
9. Normas iran ISO 17799 vr ISO 27001, 2002
10. iso 27001, 2005
11. Análisis de Riesgos. eufic.dad.be seguridad.internet2.ulsa.mx 2008
12. Guías de administración de riesgos www.esap.edu.com, 2008
13. Manual de seguridad de redes. www.arcert.gov.ar/, 2008

14. Análisis del riesgo y sistemas de gestión de seguridad de Información. www.centrum.pucep.edu.pe/., 2008
15. Normas IRAM ISO/ICE 27001Tecnologia de la Información www.icm.espol.edu.ec/materias/, 2008).(http://www.segu-info.com.ar/tesis/, 2008
16. http://es.wikipedia.org/wiki/Seguridad_inform., 2009
17. http://www.nag.ru/goodies/tia/TIA-EIA-568-B, 2009
18. Politicas de seguridad www.iec.csic.es
19. políticas y prácticas de seguridad www.rediris.es, 2007
20. Seguridad en una intranet. www.perantivirus.com
21. Políticas de seguridad 2003. www.perantivirus.com/sosvirus
22. Seguridad en la red. www.seguridadenlared.org
23. Evaluación de los Riesgos, Agustín López, Lead Auditor BS7799 certificado por BSI, 2008
24. Políticas de seguridad de la red. www.uam.es www.rediris.es, 2007
25. Gestión de seguridad de la información www.bsi-spain.com , 2007
26. www.seguridaddelainformacion.com 2007. Gestion de seguridad de la informacion.
27. www.dric.com.mx /seguridad. , 2007
28. Estándares de seguridad en la información www.unal.edu.co/seguridad, www.security.kirion.net, 2007
29. Nagios.org 2009
30. Evaluacion de nagios para linux, http://www.redextremadura.net

Anexo # 1

Ficha de Soporte Técnico del MINSA



Anexo # 2

Lineamientos de seguridad para la red de área local del MINSA –CNS

El objetivo de estos lineamientos es proveer un marco de trabajo que nos sirva de base para garantizar una protección adecuados a los equipos de cómputos, la red y de todos los datos contenidos en ellas, de amenazas proveniente tanto del exterior de la red del Ministerio de Salud (Minsa), ya sean estas intencionales o accidentales.

Con estos lineamientos, el Minsa persigue lo siguiente:

- *Garantizar que todos los equipos de cómputos* y los datos contenidos en ellos estén protegidos contra el acceso no autorizado desde adentro o fuera del MINSA.
- Garantizar que todos los usuarios del MINSA están conscientes que es su responsabilidad adherirse a éstas políticas.
- Garantizar que todos los responsables de áreas del MINSA tienen la responsabilidad de implementar estas políticas en sus respectivas áreas.
- Garantizar la integridad de los equipos de cómputo y la confidencialidad de la información contenida en ellos, es responsabilidad del área de Sistemas de Información.
- Garantizar que todos los problemas relacionados con la seguridad serán reportados al área de Sistemas de Información, para su debida investigación y solución.

1. Responsabilidades

Todos los usuarios son responsables por sus actos. El uso por parte de un usuario de los equipos y de los medios de comunicación dentro del MINSA, asume e implica que el usuario acepta estas políticas sin excepción, garantizando la seguridad e integridad de la información que los equipos contengan y que el usuario comprende sus responsabilidades.

Todos los usuarios del MINSA tienen las siguientes responsabilidades:

- Tener conocimiento y comprender correctamente todas las directrices e instrucciones contenidas en estas políticas acerca del uso apropiado de los equipos.
- Hacer uso de las características de seguridad propia de los equipos, como las contraseñas.
- Asegurar que cualquier información específica de un usuario individual, tales como, cuentas de acceso y contraseñas, son manejadas correctamente, no son compartidas y en general no se hace mal uso de ella.
- Reportar cualquier incidente relacionado a la seguridad de los equipos y la red al personal de la División de Información.

La División de Información tiene las siguientes responsabilidades:

- Asegurar que todos los responsables de áreas conozcan estas políticas, quienes a su vez deberán informar a todo su personal.
- Proveer medidas de seguridad a nivel central para proteger los equipos y la red en general de amenazas del exterior. Esto debe incluir identificación de las diferentes amenazas, provisión de herramientas y software (Antivirus, Parches, etc.) y la implementación de sistemas de seguridad como *Firewall*.
- La División de Información es responsable por las políticas de seguridad en todo el MINSA a nivel general. Entre cada una de las Divisiones del MINSA central y Unidades de Salud, la seguridad será delegada al soporte local, si existe a ese nivel, pero en completa cooperación y soporte de la División de Información del MINSA.

2. Ambiente de Computación

- La División de Sistemas de Información planifica, da mantenimiento y opera una serie de servidores, dispositivos de red, dispositivos de respaldo y todo el sistema de interconexión de los diferentes equipos de cómputo del Ministerio de Salud.
- El ambiente de computación se define como todos los recursos de cómputos y la infraestructura de red que es manejada por la División de Información y todos los dispositivos de cómputo que pueden conectarse a la red con previa autorización. Todos estos recursos están sujetos a estas políticas y
- cualquier dato que esté almacenado en estos equipos o sea accedidos a través de estos equipos dentro de la LAN y que esté relacionado con el Ministerio de Salud no importando el medio de almacenamiento (discos, CDs, cintas, etc.) en que estén almacenados.
- Cualquier conexión temporal o permanente a través de la LAN, dispositivos móviles casuales, acceso remoto por medio de modem está sujeta a estas políticas, incluyendo cualquier equipo de cómputo no perteneciente al MINSA.
- La División de Información se reserva el derecho de monitorear, registrar y analizar todas las comunicaciones en la red en cualquier momento con el propósito de diagnosticar
- Problemas de desempeño o fallas. Todo monitoreo del tráfico de la red será realizado de acuerdo a las normas nacionales e internacionales establecidas.
- El área de soporte técnico de la División de Información será el punto de contacto para cualquier solicitud de servicios de cómputo.

3. Acceso a Equipos de Cómputo

- Todos los usuarios con una **Cuenta de Usuario** válida podrán usar un equipo de cómputo dentro del Ministerio de Salud.
- Las Cuentas de Usuario son otorgadas por la División de Información y son válidas solamente para registrarse en los servidores centrales. Estas cuentas son otorgadas a usuarios individuales y no deben ser compartidas ni cedidas a otros usuarios.
- A todos los usuarios del MINSA con necesidad de tener acceso a servicios de cómputo y de comunicación, se les otorgará una cuenta de usuario con su contraseña. Las contraseñas asignadas durante la creación son de carácter temporal y deberán ser cambiadas tan pronto como sea posible.
- Las cuentas de usuario serán eliminadas en el momento en que el usuario abandone definitivamente el Ministerio.

4. Uso de Equipos en General

Se espera que todos los usuarios hagan un esfuerzo razonable para garantizar el uso apropiado de los recursos de cómputo proporcionados por el MINSA. Entre estos esfuerzos se incluyen:

- Un manejo apropiado de las cuentas de usuario y sus contraseñas.
- Un manejo apropiado de las sesiones de trabajo, como apagar correctamente el equipo al finalizar sus labores o bloquear por medio de software el equipo cuando se deja desatendido por un período de tiempo muy largo.
- Respetar las licencias o los derechos de autor del software.
- Un manejo apropiado de la información sensitiva.

5. Acceso a Internet

- Las oficinas centrales del Ministerio de Salud están conectadas a Internet a través de una conexión dedicada y cualquier usuario que cumpla con las políticas referidas en este documento puede tener acceso a este servicio.
- El acceso a Internet de los usuarios es controlado y es otorgado con previa autorización por la División de sistemas de información.

6. Correo Electrónico

- Todos los usuarios con una cuenta válida podrán enviar y recibir correo electrónico dentro y fuera del MINSA siempre y cuando hayan sido autorizados para hacerlo.
- Los usuarios no deberán usar cuentas falsificadas o mal representar a otros usuarios del MINSA en sus comunicaciones electrónicas.
- Todas las cuentas de correo tienen cuotas de espacio limitadas establecidas en ellas. Todos los buzones de correo son respaldados regularmente.
- Toda la comunicación a través del correo electrónico dentro y fuera del MINSA será revisada para garantizar que no contengan virus o cualquier otra forma de código malicioso conocido. Estos correos infectados pueden ser bloqueados y se le retornará al usuario con la información necesaria para realizar su desinfección.

7. Acceso a la Red de área local:

- La mayoría de los empleados del Minsa necesitan acceso a la red, antes de que un equipo sea conectado a la red, los usuarios deberán solicitar la autorización al soporte local, el cual proporcionara la información necesaria para que la conexión pueda realizarse.

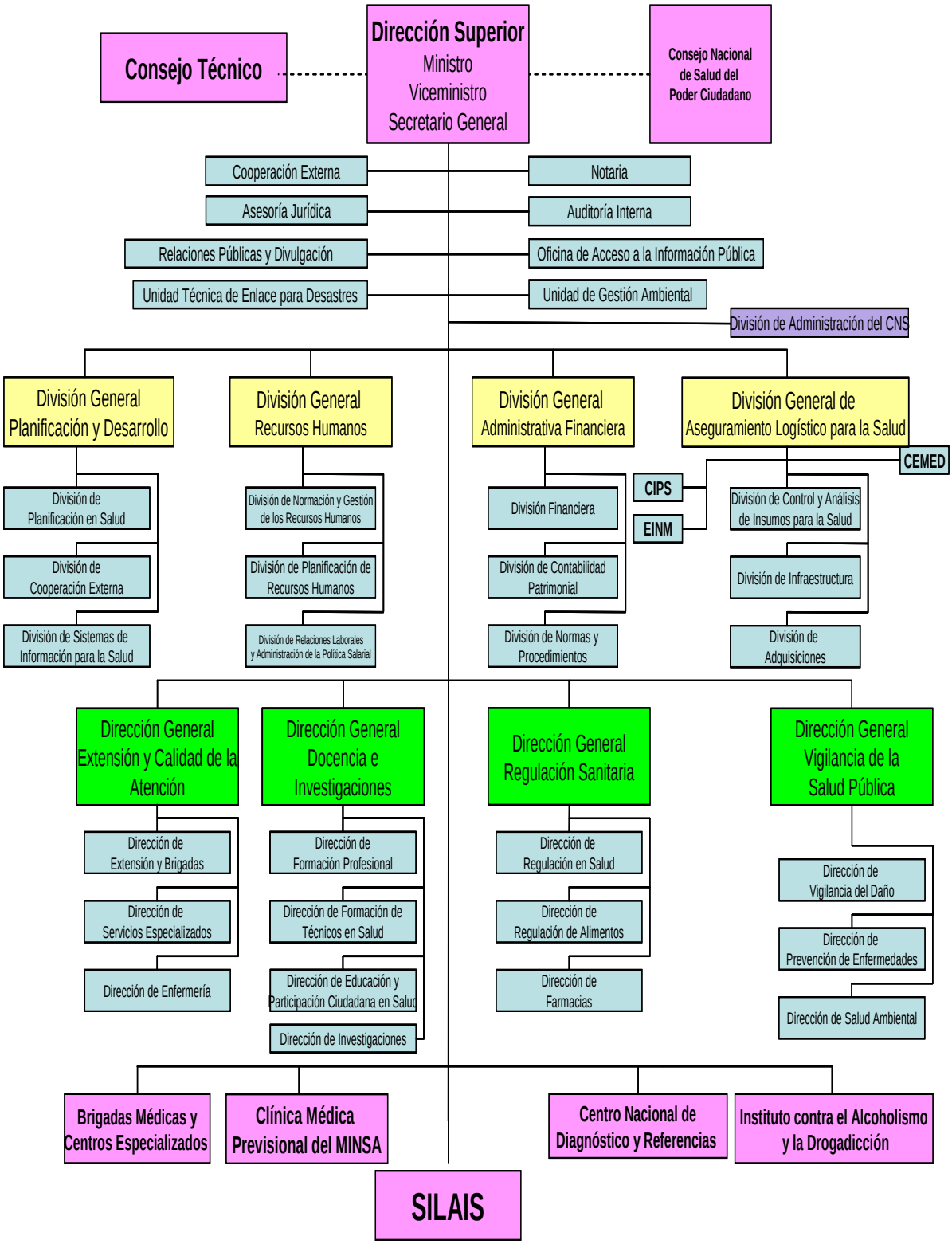
- Los usuarios no deben de leer ni copiar información sensitiva aunque esté disponible para ellos (por un mal uso de los privilegios). Cuando se descubra este tipo de información, los usuarios deberán información, los usuarios deberán informar a la División de Sistemas para que tomen las medidas pertinentes.

8. Programas Informáticos:

- La División de Sistemas de Información proveerá los medios a través de los cuales los usuarios podrán copiar e instalar los diferentes tipos de programas informáticos (aplicaciones y herramientas) necesarias para realizar sus labores diarias.
- Los usuarios no están autorizados a instalar ningún programa informático que no hayan sido previamente aprobados por la División de Sistemas de Información.

Anexo 3

Organigrama 2009 Ministerio de Salud



Anexo # 4

Manual de funciones de la División de Sistemas de Información

Ficha Ocupacional 1		
EMISION:	**DIVISION:** Informática	**APROBADO POR:** División de sistemas de Información
DESCRIPCIÓN DE CARGO DE TRABAJO		
Dependencia Organizativa	Administración de la Información.	
Nombre del Cargo	Administrador de la red LAN	
Cargo Superior Inmediato	Responsable del tecnología de información y comunicación(TIC)	
Cargos Subordinados	Ninguno	
Propósito del Cargo Planificación, Organización y Mantenimiento de la infraestructura de datos e Internet necesarios para la conectividad a la Intranet e Internet del Ministerio de Salud. (Backbone alambrado e inalámbrico)		
FUNCIONES		
1	Asigna los permisos para navegar por la red, correo electrónico.	
2	Controla los IP de cada usuario del Ministerio de Salud.	
3	Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo.	
4	Hacer la red más segura, protegiéndola contra el acceso no autorizado, haciendo imposible que personas ajena pueda entender la información que circule en ella.	
5	Controlar cambios y actualizaciones en la red de modo que ocasionen las menos interrupciones posibles, en el servicio a los usuarios.	
6	Analiza los parámetros para obtener conclusiones que permitan deducir rápidamente lo que pasa en la red.	
7	Asegurar el funcionamiento de las redes para una transmisión de datos consistente, eficiente, segura con parámetros medibles y reportables de carácter internacional y debidamente documentados.	
8	Medir y reportar el funcionamiento de la red, identificar áreas problemáticas, aislar la naturaleza exacta de los problemas, restituir la red.	
9	Realiza y Lleva un control sobre el mantenimiento y rendimiento de los sistemas ya existentes.	
10	Asistir y auxiliar en la configuración de equipos del Centro de Operación de Red y Comunicación a INTERNET.	

11	Administrar el control de acceso a la Red de servicios de INTERNET implicando el registro, archivo y actualización de los datos de información de la Red.
12	Elabora y entrega al jefe inmediato informe mensual, trimestral, semestral y anualmente del avance de todo lo relacionado con su Plan Operativo individual y del cumplimiento de sus funciones.
13	Cumple los reglamentos, normas y disposiciones del Ministerio de Salud que le corresponden.
14	Realiza todas aquellas tareas que le son delegadas por su jefe inmediato relacionadas con el área.
Relaciones principales con otros Cargos ➢ **División General de planificación y Desarrollo.**	
Relaciones principales con otras Organizaciones y/o Instituciones ➢ Ninguna	
Perfil del Cargo	
Conocimientos requeridos fundamentales ➢ Dominio de dos o más lenguajes de programación.	
Formación básica **Nivel y especialización** ➢ Graduado Universitario ➢ Ingeniero de Sistemas o en Computación ➢ Con estudios de Post Grado en Sistemas de Información	
Conocimiento específico ➢ Comunicación verbal y escrita ➢ Buenas relaciones humanas ➢ Utilización de informática: Programa de procesamientos de texto y hoja de cálculo en ambiente Windows ➢ Manejo de herramientas de software case ➢ Manejo de sistema de bases de datos distribuidos ➢ Manejo de tecnología orientada a objetos ➢ Utilización de la informática a nivel de Redes Locales e Internet	
Conocimientos deseables ➢ Bilingüe	
Experiencia **Tipo de Experiencia y años** ➢ En cargos similares ➢ Con dos años de experiencia	
Otros requisitos ➢ Manejo de información confidencial ➢ Ética profesional ➢ Capacidad de trabajo en equipo	

Tabla Nº 1 ficha ocupacional de la Administración de Información

Ficha Ocupacional 2		
EMISION:	**DIVISION:** Informática	**APROBADO POR:** División de Sistemas de Información

DESCRIPCIÓN DE CARGO DE TRABAJO	
Dependencia Organizativa	Administración de la Información.
Nombre del Cargo	Asistente
Cargos Subordinados	Ninguno

Propósito del Cargo

Maneja la documentación del área, lleva agenda de trabajo de su jefe inmediato, así como en las coordinaciones delegadas por el jefe superior.

FUNCIONES	
1	Recibe, registra, clasifica, ordena y archiva correspondencia que llega a su oficina; contesta y distribuye correspondencias en las otras dependencias del área Informática del Ministerio de Salud.
2	Atiende visitas del personal externo del Minsa, evacua consultas y brinda las orientaciones a los mismos sobre los diferentes procedimientos en las gestiones que éstos realizan en su área de ubicación.
3	Asiste en reuniones a su jefe inmediato y toma nota de todo lo referente a temas tratados, transcribe el acta o informe requerido, lo hace llegar a las instancias correspondientes.
4	Atiende y efectúa llamadas telefónicas tanto locales e internacionales, recibe y brinda información, así como anota mensajes y los transmite al jefe inmediato.
5	Elabora solicitudes de papelería y útiles de oficina cuando se requiera; además de recibirla y se encarga de controlar, resguardar y distribuir al personal de su área.
6	Realiza redacción de documentos que sean orientadas por el jefe superior.
7	Controla, ordena, resguarda y mantiene actualizado el archivo de su jefe inmediato para agilizar la localización de la información y documentación del su área.
8	Fotocopia y encolocha documentos que se le sean encomendados.
9	Asiste al personal ubicado en su área en los aspectos de correspondencia.
10	Coordina actividades en las que participará el responsable del área, en cuanto a programación (fecha, hora, lugar, áreas y participantes).
11	Cumple los reglamentos, normas y disposiciones del Ministerio de Salud que corresponden al personal.

12	Realiza tareas delegadas por su jefe inmediato, relacionadas con el área.

Relaciones principales con otros cargos

- Asistentes y Secretarias de las distintas áreas del Ministerio de salud.

Relaciones principales con otras organizaciones y/o Instituciones

- Instituciones del estado

Perfil del Cargo

Conocimientos requeridos fundamentales

- Redacción
- Informática

Formación básica

Nivel y especialización

- Graduada de Secretaria Ejecutiva
- Operador de Microcomputadora

Conocimiento específico

- Técnicas de redacción de informes
- Técnicas de archivo
- Comunicación verbal y escrita
- Relaciones humanas
- Utilización de Procesador de texto, Hojas de cálculo y Diseñador de presentaciones

Conocimientos deseables

- Bilingüe
- Utilización de informática al nivel de Redes Locales

Experiencia

Tipo de experiencia y años

- **Cargos similares**
- **Con mínimo dos años de experiencia**

Otros requisitos

- **Confidencial**
- **Ética Profesional**
- **Capacidad de trabajo bajo presión**

Tabla Nº 2 ficha ocupacional de la Asistente

Ficha Ocupacional 3		
EMISION:	**DIVISION:** Informática	**APROBADO POR:** División de sistemas de Información
DESCRIPCIÓN DE CARGO DE TRABAJO		
Dependencia Organizativa	Administración de la Información.	
Nombre del Cargo	Administrador de la red LAN	
Cargo Superior Inmediato	Responsable del tecnología de información y comunicación(TIC)	
Cargos Subordinados	Ninguno	
Propósito del Cargo Planificación, Organización y Mantenimiento de la infraestructura de datos e Internet necesarios para la conectividad a la Intranet e Internet del Ministerio de Salud. (Backbone alambrado e inalámbrico)		
FUNCIONES		
1	Asigna los permisos para navegar por la red, correo electrónico.	
2	Controla los IP de cada usuario del Ministerio de Salud.	
3	Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo.	
4	Hacer la red más segura, protegiéndola contra el acceso no autorizado, haciendo imposible que personas ajena pueda entender la información que circule en ella.	
5	Controlar cambios y actualizaciones en la red de modo que ocasionen las menos interrupciones posibles, en el servicio a los usuarios.	
6	Analiza los parámetros para obtener conclusiones que permitan deducir rápidamente lo que pasa en la red.	
7	Asegurar el funcionamiento de las redes para una transmisión de datos consistente, eficiente, segura con parámetros medibles y reportables de carácter internacional y debidamente documentados.	
8	Medir y reportar el funcionamiento de la red,	
9	Atender las solicitudes de usuarios en casos de encontrar problemas de enlace con la red de servicio de INTERNET/INTERNET del Ministerio de Salud.	
10	Administrar el control de acceso a la Red de servicios de INTERNET implicando el registro, archivo y actualización de los datos de información de la Red	
11	Elabora y entrega al jefe inmediato informe mensual, trimestral, semestral y anualmente del avance de todo lo relacionado con su Plan Operativo individual y del cumplimiento de sus funciones	

Relaciones principales con otros Cargos ➢ **División General de planificación y Desarrollo.**
Relaciones principales con otras Organizaciones y/o Instituciones ➢ Ninguna
Perfil del Cargo
Conocimientos requeridos fundamentales ➢ Dominio de dos o más lenguajes de programación.
Formación básica **Nivel y especialización** ➢ Graduado Universitario ➢ Ingeniero de Sistemas o en Computación ➢ Con estudios de Post Grado en Sistemas de Información
Conocimiento específico ➢ Comunicación verbal y escrita ➢ Buenas relaciones humanas ➢ Utilización de informática: Programa de procesamientos de texto y hoja de cálculo en ambiente Windows ➢ Manejo de herramientas de software ➢ Manejo de sistema de bases de datos distribuidos ➢ Manejo de tecnología orientada a objetos ➢ Utilización de la informática a nivel de Redes Locales e Internet
Conocimientos deseables ➢ Bilingüe
Experiencia **Tipo de Experiencia y años** ➢ En cargos similares ➢ Con dos años de experiencia
Otros requisitos ➢ Manejo de información confidencial ➢ Ética profesional ➢ Capacidad de trabajo en equipo

Tabla Nº 3 ficha ocupacional de la administración de información

Ficha Ocupacional 4		
EMISION:	**DIVISION:** Informática	**APROBADO POR:** División de sitemas de Información.
DESCRIPCIÓN DE CARGO DE TRABAJO		
Dependencia Organizativa	Administración de la Información.	
Nombre del Cargo	Asistente	
Cargos Subordinados	Ninguno	
Propósito del Cargo Maneja la documentación del área, lleva agenda de trabajo de su jefe inmediato, así como en las coordinaciones delegadas por el jefe superior.		
FUNCIONES		
1	Recibe, registra, clasifica, ordena y archiva correspondencia que llega a su oficina; contesta y distribuye correspondencias en las otras dependencias del área Informática del Ministerio de Salud.	
2	Atiende visitas del personal externo del Minsa, evacua consultas y brinda las orientaciones a los mismos sobre los diferentes procedimientos en las gestiones que éstos realizan en su área de ubicación.	
3	Asiste en reuniones a su jefe inmediato y toma nota de todo lo referente a temas tratados, transcribe el acta o informe requerido, lo hace llegar a las instancias correspondientes.	
4	Atiende y efectúa llamadas telefónicas tanto locales e internacionales, recibe y brinda información, así como anota mensajes y los transmite al jefe inmediato.	
5	Elabora solicitudes de papelería y útiles de oficina cuando se requiera; además de recibirla y se encarga de controlar, resguardar y distribuir al personal de su área.	
6	Realiza redacción de documentos que sean orientadas por el jefe superior.	
7	Controla, ordena, resguarda y mantiene actualizado el archivo de su jefe inmediato para agilizar la localización de la información y documentación del su área.	
8	Fotocopia y encolocha documentos que se le sean encomendados.	
9	Asiste al personal ubicado en su área en los aspectos de correspondencia, comunicaciones, fotocopias.	

10	Coordina actividades en las que participará el responsable del área, en cuanto a programación (fecha, hora, lugar, áreas y participantes).
11	Cumple los reglamentos, normas y disposiciones del Ministerio de Salud que corresponden al personal.
12	Realiza tareas delegadas por su jefe inmediato, relacionadas con el área.

Relaciones principales con otros cargos

- Asistentes y Secretarias de las distintas áreas del Ministerio de salud.

Relaciones principales con otras organizaciones y/o Instituciones

- Instituciones del estado

Perfil del Cargo

Conocimientos requeridos fundamentales

- Redacción
- Informática

Formación básica

Nivel y especialización

- Graduada de Secretaria Ejecutiva
- Operador de Microcomputadora

Conocimiento específico

- Técnicas de redacción de informes
- Técnicas de archivo
- Comunicación verbal y escrita
- Relaciones humanas
- Utilización de Procesador de texto, Hojas de cálculo y Diseñador de presentaciones

Conocimientos deseables

- Bilingüe
- Utilización de informática al nivel de Redes Locales

Experiencia

Tipo de experiencia y años

- **Cargos similares**
- **Con mínimo dos años de experiencia**

Otros requisitos

- **Confidencial**
- **Ética Profesional**
- **Capacidad de trabajo bajo presión**

Tabla Nº 4 ficha ocupacional de la Asistente

Anexo # 5

Complejo Nacional de Salud Dra. Concepción Palacios

Ministerio de Salud

Entrevista Administradores de la red

1. Normas de seguridad

1.1 ¿Existe un documento disponible de Normas de seguridad para todos los usuarios?

Si ( )

No ( )

1.2 ¿Cuál de los aspectos siguientes, considera usted que, inciden en que no haya un documento tecnológico sobre Seguridad?

a) Presupuesto ( )
b) Tiempo ( )
c) Cultura organizacional ( )
d) Desconocimiento ( )

2. Seguridad física del Entorno

2.1 El edificio donde se encuentra los activos de redes están a salvo de:

a) Inundación ( )
b) Robos ( )
c) Polvo ( )
d) Fluctuación de Energía ( )

2.2 ¿Están las áreas protegidas por controles físicos de entrada para permitir el acceso solo al personal autorizado?

Si ( )

No ( )

3. Tecnología de comunicaciones

3.1 Disponen de las siguientes tecnologías?

a) Ordenadores ( )
b) Intranet ( )
c) Red de área local (LAN) ( )
d) Extranet ( )

4. Clasificación y control de los activos de red

4.1. ¿El área de informática tiene un software para el control de inventario de los equipos conectados a red?

Si ( )

No ( )

4.2. ¿Se registran las actividades de los operadores para evitar que realicen un mal funcionamiento en los activos de red que pueda dañar los sistemas?

Si ( )

No ( )

4.3. ¿La Oficina de Informática, mantiene actualizados los inventarios de los activos de red?

Si ( )

No ( )

5. Incidentes de seguridad

5.1 ¿Hay un canal en que los usuarios reporten los incidentes de seguridad tales como?

a) Problemas con el Sistemas Operativos ( )
b) Debilidades o amenazas al sistema ( )
c) Fallos de software ( )
d) Fallas de PC y portátiles ( )

5.2 ¿Existen proceso disciplinario para tratar las violaciones de seguridad realizadas por los usuarios del Ministerio?

Si ( )

No ( )

5.3 ¿Han realizado algún estudio sobre amenazas de seguridad y su costo?

Si ( )

No ( )

6. Seguridad en las instalaciones de la red

6.1 ¿Qué medidas de seguridad poseen las instalaciones de la red?

a) Seguridad del equipamiento ( )
b) Aire acondicionado ( )
c) Ventanales protegidos contra la luz solar ( )
d) Equipos contra incendios ( )
e) Suministro de energía ( )
f) Protección del cableado eléctrico ( )

6.2 La seguridad de la red está en manos de:

a) Una persona ( )
b) Dos personas ( )
c) Tres personas ( )

6.3 ¿Que casos de violaciones de seguridad ha tenidos los activos de red?

a) Manipulación de aplicaciones de software. ( )

b) Acceso no autorizado a la Web.( )

c) Robos de dato ( )

d) Virus ( )

e) Pérdida de la información. ( )

6.4 ¿La institución cuenta con asesorías externas en medidas de seguridad en la red?

Si ( )

No ( )

7. Seguridad en la red

7.1 ¿Cuáles de los siguientes mecanismos utiliza actualmente su institución para proteger sus sistemas de información?

a) Antivirus. ( )
b) Contraseñas. ( )
c) Firewalls hardware. ( )
d) Firewalls software. ( )
e) Sistemas de detección de intrusos. ( )

8. Gestión de Comunicación

8.1 ¿Qué tipo de conexión posee la red LAN?

Seleccione una:

a) Conmutada ( )
b) Dedicada Vía radio ( )
c) Fibra Óptica ( )

8.2 ¿Utiliza Switch en su red LAN?

Si ( )

No ( )

8.3 ¿Utiliza Ruteadores al interior de tu Red?

Si ( )

No ( )

9. Protección contra software malicioso

9.1 ¿Disponen de las herramientas tales como?

a) Sistemas de detección de intrusos. ( )
b) Corta fuego (firewall) (software o hardware) ( )
c) Monitorización de red o sniffer. ( )
d) Encriptación de datos para su confidencialidad. ( )
e) Firma electrónica digital. ( )
f) Pass Word/ login. ( )

9.2 ¿Posee de licencias de antivirus corporativos actualizados?

Si ( )

No ( )

9.3 ¿Los software antivirus protegen, correos y las descargas de archivos adjuntos?

Si ( )

No ( )

9.4 ¿Actualiza regularmente su antivirus?

Si ( )

No ( )

9.5 ¿Disponen de antivirus para los servidores de ficheros?

Si ( )

No ( )

9.6 ¿Disponen de antivirus los servidores de aplicación. ?

Si ( )

No ( )

9.7 ¿Disponen de antivirus los servidores de correos. ?

Si ( )

No ( )

10. Administración

10.1 ¿Se hacen regularmente copias de seguridad?

Si ( )

No ( )

10.2. ¿Se reportan los fallos del sistema y se toman medidas correctivas?

Si ( )

No ( )

11. Control de acceso de los usuarios

11.1 ¿Existe un proceso para la gestión de pasword?

Si ( )

No ( )

11.2 ¿Se revisan periódicamente los derechos de acceso de los usuarios?

Si ( )

No ( )

12. Control de acceso a la red:

12.1 ¿Qué herramienta utiliza para administrar la red de telecomunicaciones del Ministerio de Salud?

1. Software para administrar la red ( )
2. Manual ( )

12.2 ¿Dispone la Institución de E-mail?

Si ( )

No ( )

12.3 ¿Existe una Norma de seguridad para los accesos a Internet y correo electrónico?

Si ( )

No ( )

12.4 ¿Está limitado el acceso a Internet por usuarios?

Si ( )

No ( )

12.5 ¿Exciten un control sobre las paginas que accede los usuarios por Internet?

Si ( )

No ( )

13. Riesgos lógicos de comunicación:

13.1. ¿Existen algunos problemas de seguridad lógicos en la red cómo?

a) Duplicados de IP ( )
b) Virus informáticos ( )
c) Caída de la red ( )

14. Seguridad de los sistemas:

14.1 ¿Están definidas las responsabilidades para proteger y controlar la información de los sistemas?

Si ( )

No ( )

14.2 ¿Tiene la institución un especialista en seguridad de redes?

Si ( )

No ( )

14.3 ¿Poseen una herramienta de seguridad para monitorear los servicio y equipos conectados a la red LAN?

Si ( )

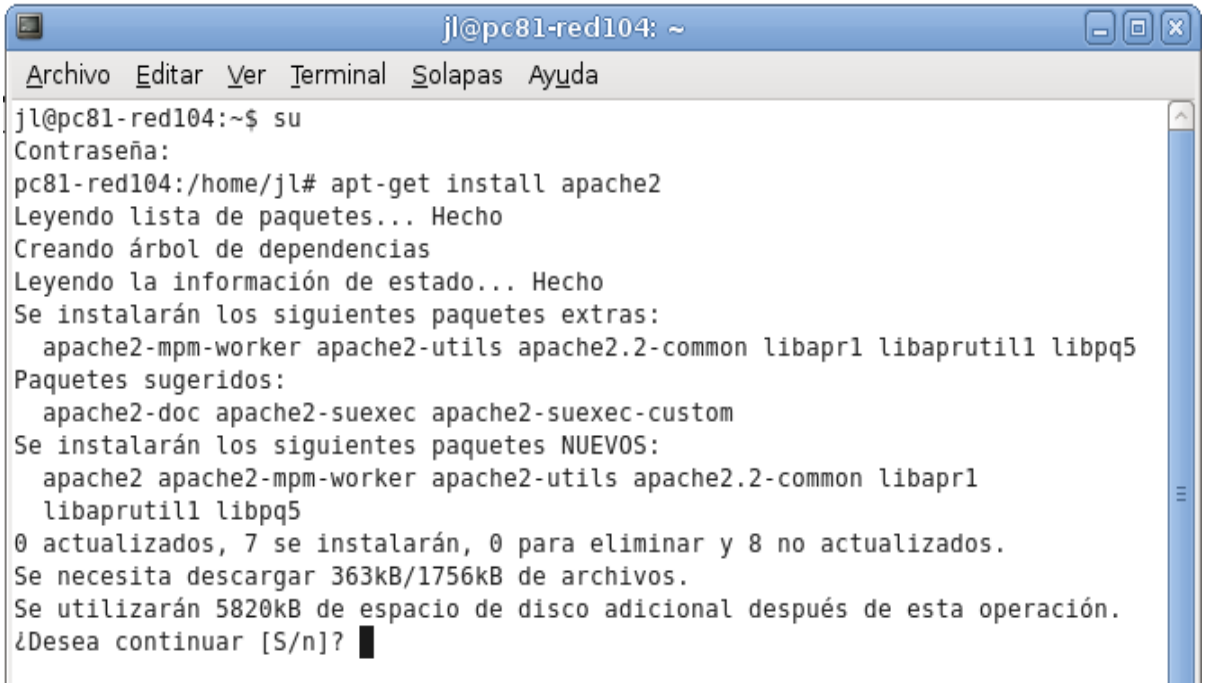
No ( )

Anexo # 6

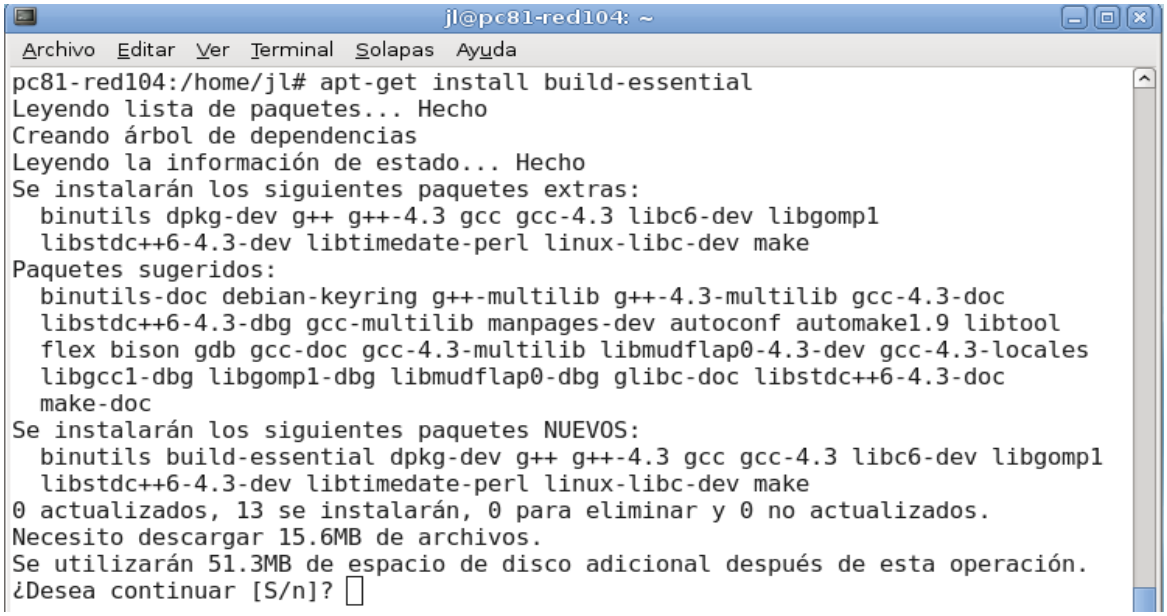
MANUAL DE INSTALACION DE NAGIOS
PARA EL MONITOREO DE LA RED DE DATOS DEL MNINSTERIO DE SALUD

1. Requerimientos de Software:

Tenemos que tener instalado en una computadora el Sistema Operativo Debian5 Lenny versión 32bits.Se necesita tener instalado y configurado un servidor web Apache. Ubicados en la consola como root escribimos en siguiente comando con el cual instalaremos apache desde los repositorios: **apt-getinstall apache2**

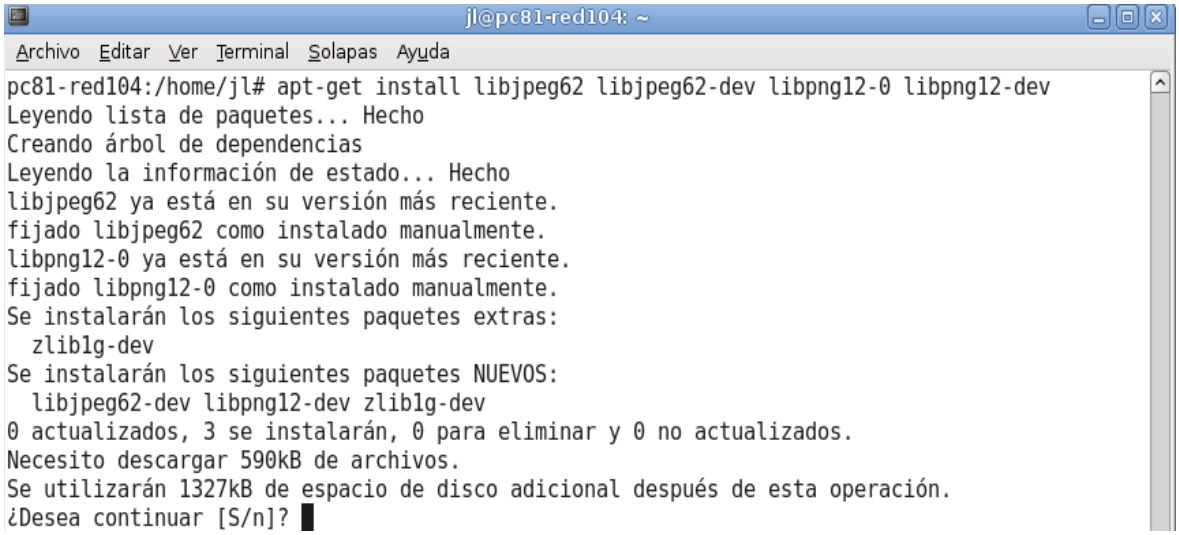


2. Instalamos nuestro entorno de compilación, este paquete tiene todo lo necesario: **apt-getinstallbuild-essential**



3. Instalamos bibliotecas necesarias para imágenes como: JPEG, PNG, GD2 para las imágenes que usara Nagios en su mapa de estado con el siguiente comando:

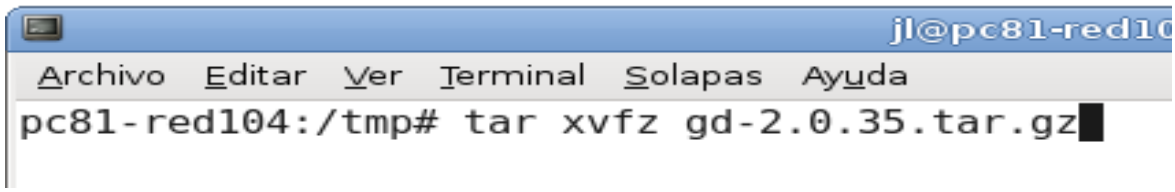
OpenGL Shaders not sup **apt-get install libjpeg62 libjpeg62-dev libpng12-0 libpng12-dev**



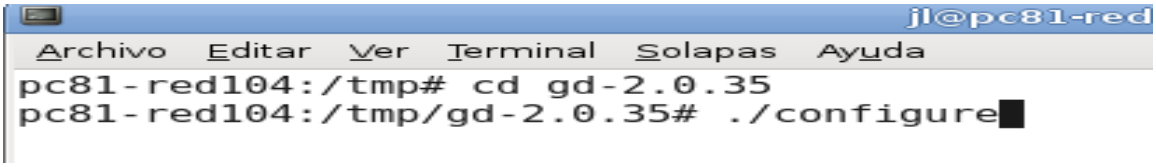
También necesitamos tener instalados la librería GD por lo tanto descargaremos las fuentes: Nos ubicamos en el directorio **tmp** como se muestra en la imagen cd /tmp en la consola de Linux.

4. Luego descargamos la última versión las fuentes con la ayuda del gestor de descarga wget de Linux como en la siguiente figura: **wget -c** http://www.libgd.org/realeses/gd-2.0.35.tar.gz

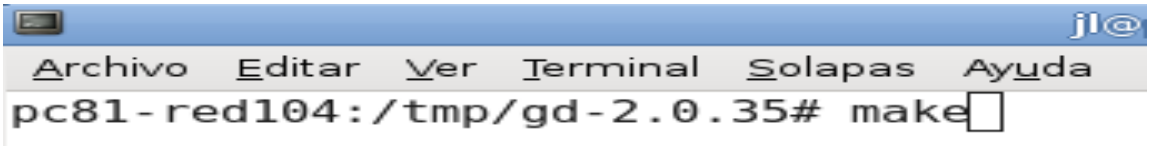
Una vez descargada la librería gd, hay que proceder a descomprimirla:



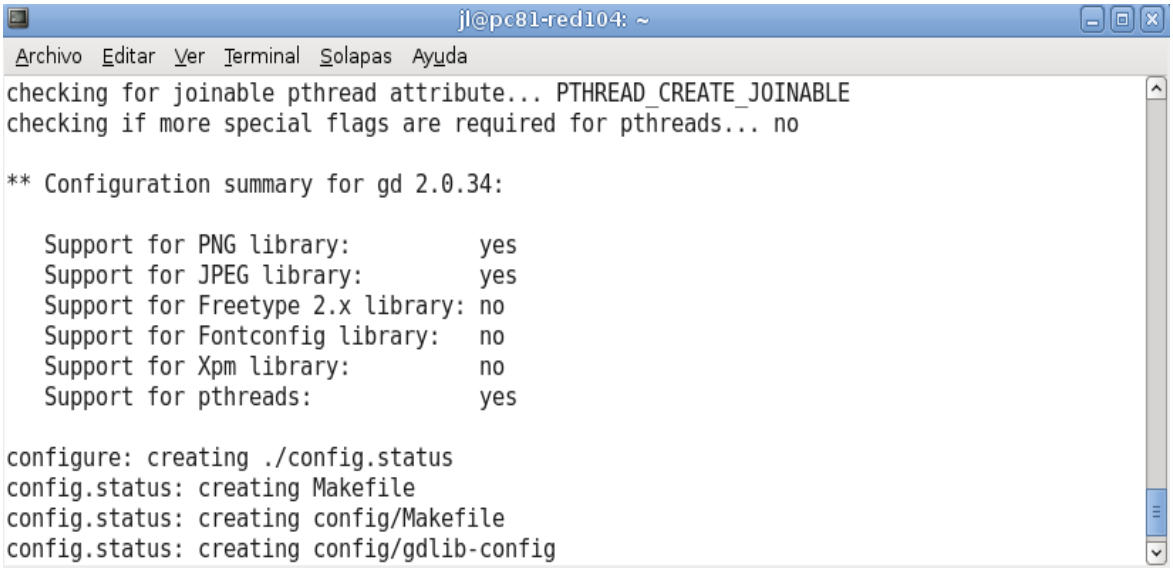
Ahora hay que ubicarse en la carpeta resultante del proceso de descompresión y después configuramos la librería con la instrucción. /**configure** como se observa OpenGL Shadersnotsupen la imagen.



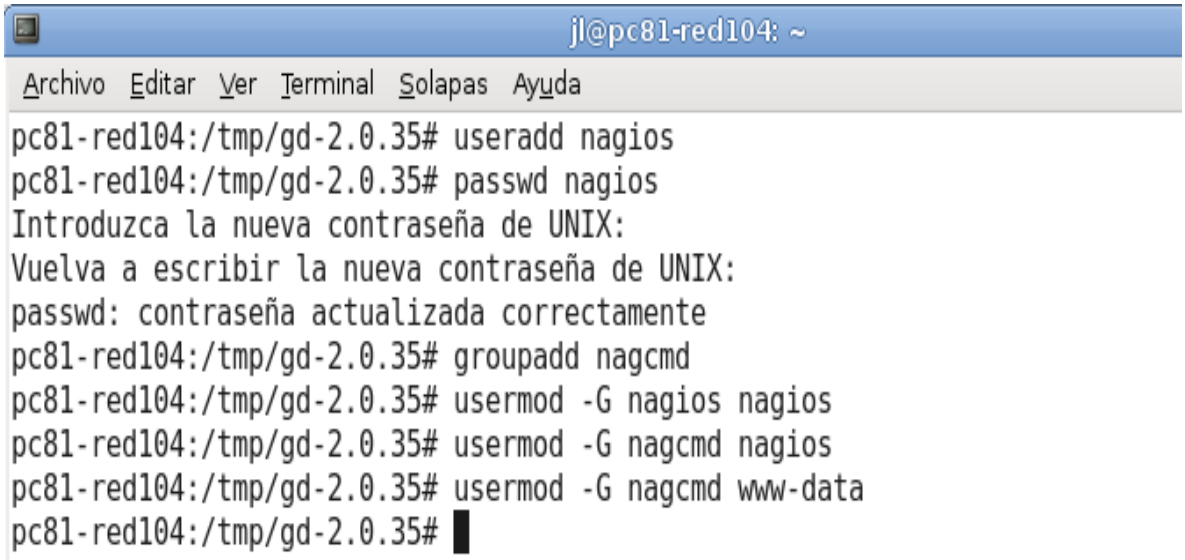
Una vez configurado se procede a compilarse con el comando **make**.



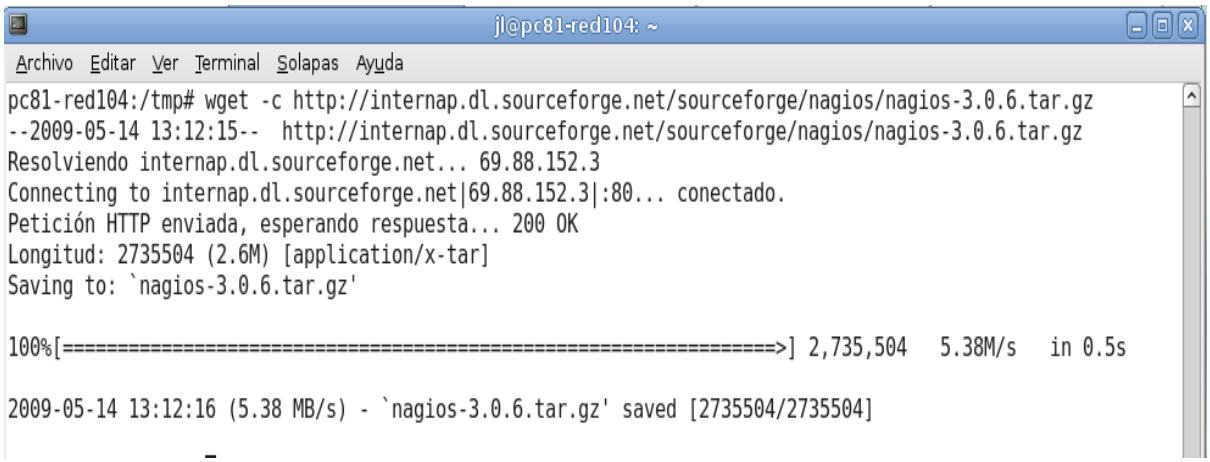
Ahora lo instalamos con el comando **makeinstall** y esta es su salida.



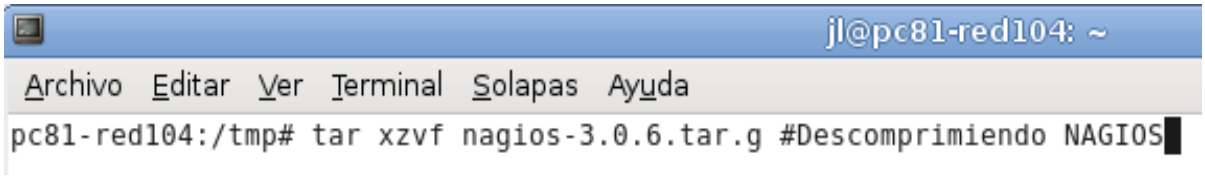
5. Ahora se crea el usuario Nagios y el grupo:



6. Ahora se descarga Nagios-3.0.6 utilizando el gestor de descarga wget en la consola siempre ubicada en la carpeta /tmp:wget -c http://internap.dl.sourceforce.net/sourceforce/nagios/nagios-3.0.6.tar.gzcomo se ve en la figura:

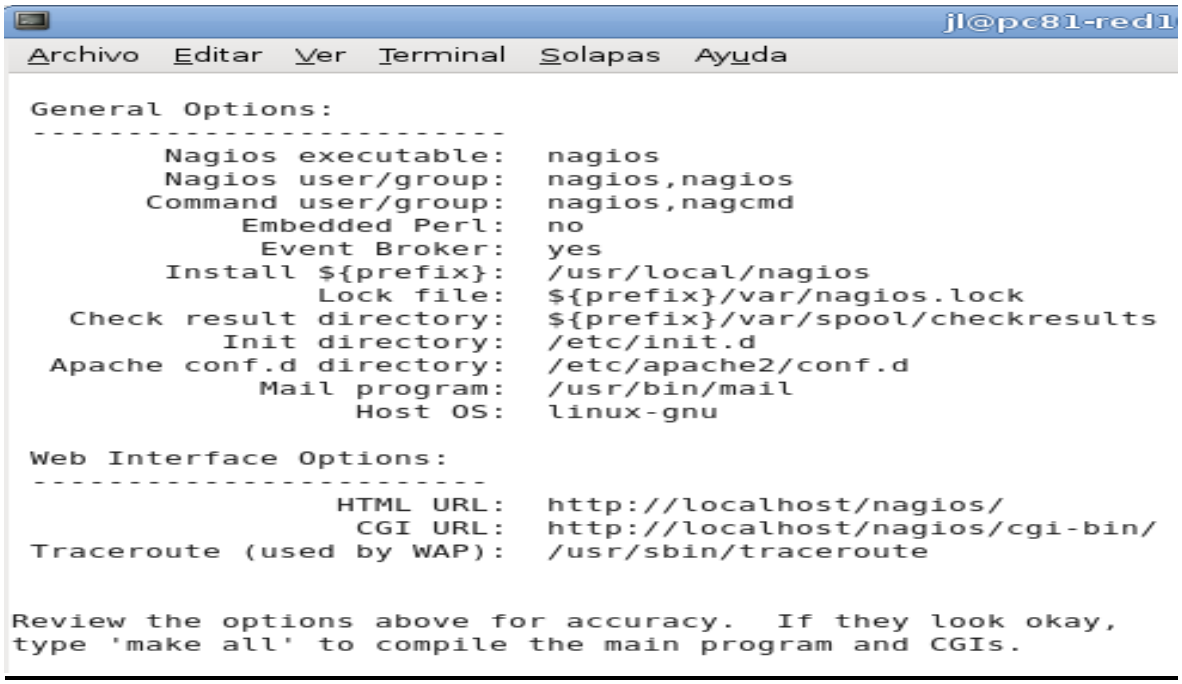


7. Después de haberlo descargado hay que proceder a descomprimir las fuentes de la siguiente forma:



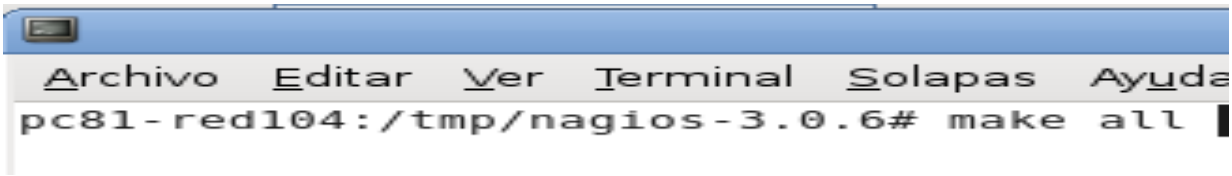
8. Ahora nos ubicamos en la carpeta descomprimida nagios-3.0.6 y pasamos a correr el scrip de configuración y agregamos a este el grupo que creamos anteriormente:

9. La salida al correr el scrip de configuración nos mostrara las opciones que tendremos al instalar Nagios en nuestro Sistema Operativo que mostrare en la siguiente página.



10. En la imagen anterior se muestra las direcciones de los directorios de configuración de Nagios tanto web como para administrar Nagios.

Ahora procederemos a compilar las fuentes de Nagios:

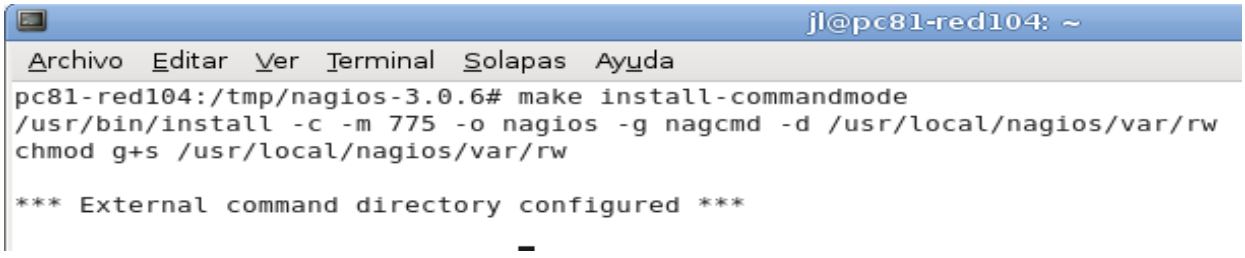


```
*** Main program, CGIs and HTML files installed ***

You can continue with installing Nagios as follows (type 'make'
without any arguments for a list of all possible options):

  make install-init
     - This installs the init script in /etc/init.d

  make install-commandmode
     - This installs and configures permissions on the
       directory for holding the external command file

  make install-config
     - This installs sample config files in /usr/local/nagios/etc

make[1]: se sale del directorio `/tmp/nagios-3.0.6'
```

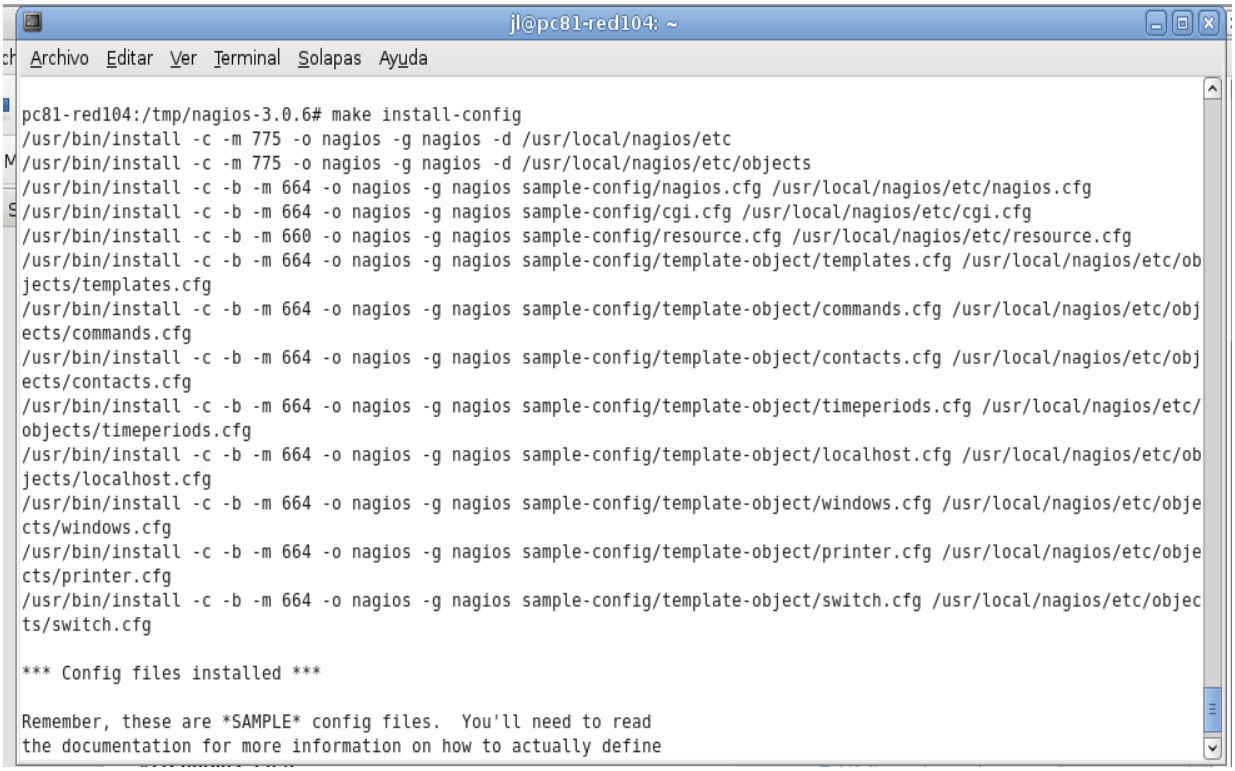
11. Una vez compilado se procede a la instalación del initscrip de Nagios como se ve en la siguiente imagen:

```
pc81-red104:/tmp/nagios-3.0.6# make install-init
/usr/bin/install -c -m 755 -d -o root -g root /etc/init.d
/usr/bin/install -c -m 755 -o root -g root daemon-init /etc/init.d/nagios
```

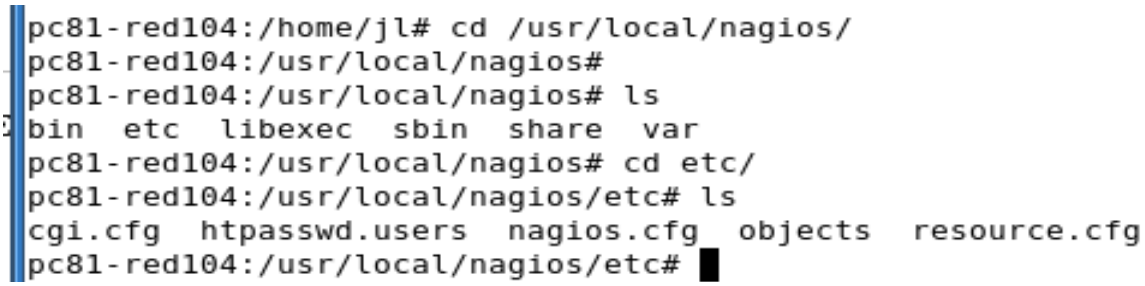
12. Ahora se instala los permisos para que se ejecuten comandos externos en el directorio Nagios.



13. Instalamos los archivos de conjuración de Nagios con: **makeinstall-config** como se muestra en la siguiente imagen:



14. El resultado del comando son los archivos de configuración de Nagios que se encuentran en **/usr/local/nagios/etc** como se muestra en la siguiente figura.



Como son **cgi.cg,** en ese archivo esta la configuración **Interfaz de entrada común** (en inglés *Common Gateway Interface*, abreviado **CGI**) es una importante tecnología de la Worl Wide Webque permite a un cliente (explorador web) solicitar datos de un programa ejecutado en un servido rweb. CGI especifica un estándar para transferir datos entre el cliente y el programa.

Para mayor referencia visite:

http://es.wikipedia.org/wiki/Common_Gateway_Interface

Contiene la configuración de la alertas de sonido que tiene Nagios por defecto, también los permisos de ejecución que tiene el usuario administrador de Nagios, etc.

Ejemplo del contenido del archivo antes mencionado:

SOUND OPTIONS

These options allow you to specify an optional audio file

that should be played in your browser window when there are

problems on the network. The audio files are used only in

the status CGI. Only the sound for the most critical problem

will be played. Order of importance (higher to lower) is as

follows: unreachable hosts, down hosts, critical services,

warning services, and unknown services. If there are no

visible problems, the sound file optionally specified by

'normal_sound' variable will be played.

<varname>=<sound_file>

#

Note: All audio files must be placed in the /mediasubdirectory

under the HTML path (i.e. /usr/local/nagios/share/media/).

#host_unreachable_sound=hostdown.wav

#host_down_sound=hostdown.wav

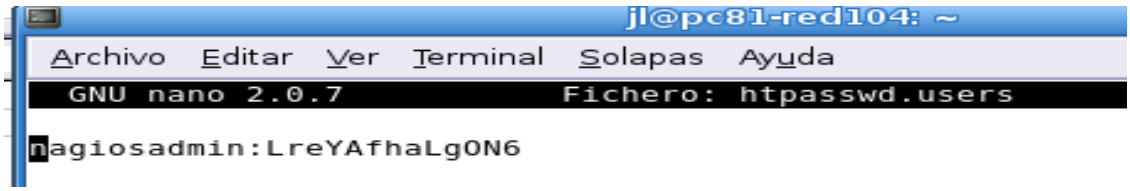
#service_critical_sound=critical.wav

#service_warning_sound=warning.wav

#service_unknown_sound=warning.wav

#normal_sound=noproblem.wav

15. El archivo **htpasswd.users** es donde está contenido la clave del usuario Nagios que es **nagiosadmin** y la contraseña encriptado como se ve en la imagen a continuación.



El Archivo nagios.cfg contiene la configuración de Nagios para agregar los archivos de los host a

Nagios en su interfaz web.

LOG FILE

This is the main log file where service and host events are logged

for historical purposes. This should be the first option specified

intheconfig file!!!

log_file=/usr/local/nagios/var/nagios.log # especifica el archivos de los log de Nagios

También contiene la definición de los archivos de los host que Nagios monitorea:

Definitions for monitoring the local (Linux) host

cfg_file=**/usr/local/nagios/etc/objects/localhost.cfg**

Archivo de definición de host local

Definitions for monitoring a Windows machine

#cfg_file=**/usr/local/nagios/etc/objects/windows.cf**g

Archivo de definición de host windows

Definitions for monitoring a router/switch

#cfg_file=**/usr/local/nagios/etc/objects/switch.cfg**

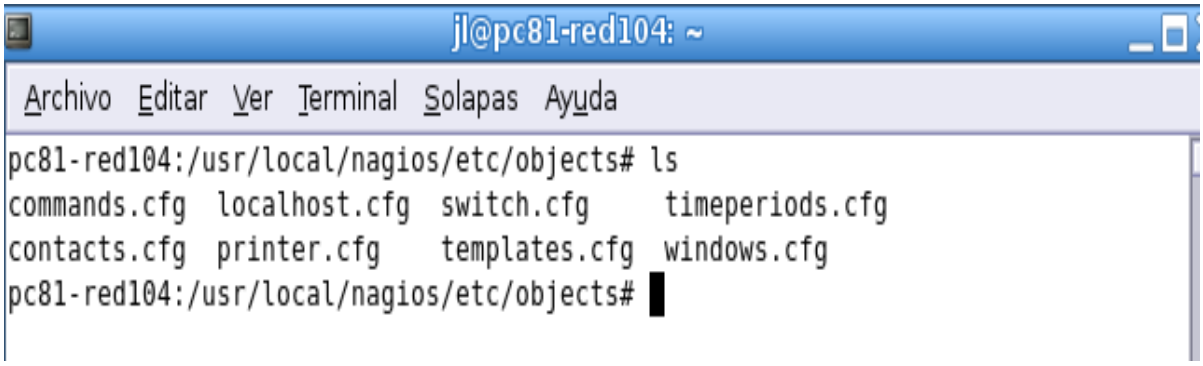
Archivo de definición de switch

Definitions for monitoring a network printer

#cfg_file=**/usr/local/nagios/etc/objects/printer.cfg**

Archivo de definición de impresoras de red.

16. En el directorio **objects** se pude encontrar los ejemplos que se instalan de definición de host y el archivo de definición de plugin como lo es el **command.cfg**, el de definición de contactos**contacts.cfg**, etc .



El contenido del archivo localhost.cfg es donde se define las propiedades del equipo en el cual corre Nagios como se muestra a continuación:

##
##############

LOCALHOST.CFG - SAMPLE OBJECT CONFIG FILE FOR MONITORING THIS

MACHINE

#

```
# Last Modified: 05-31-2007
#
# NOTE: This config file is intended to serve as an *extremely* simple
# example of how you can create configuration entries to monitor
# the local (Linux) machine.
#
##############################################################################
##############################################################################
##############################################################################
#
# HOST DEFINITION
#
##############################################################################
##############################################################################
# Define a host for the local machine
define host{
uselinux-server
; Name of host template to use
                ; This host definition willinhe variables that are defined
; in (or inherited by) the linux-server hosttemplate definition.
```

```
host_namelocalhost
aliaslocalhost
address 127.0.0.1
      }
##############################################################################
#
# HOST GROUP DEFINITION
#
##############################################################################
# Define an optional hostgroup for Linux machines
definehostgroup{
hostgroup_namelinux-servers ; The name of the hostgroup
alias Linux Servers ; Long name of the group
memberslocalhost ; Comma separated list of hosts that belong to this group
}
##############################################################################
##############################################################################
```

```
#
# SERVICE DEFINITIONS
#
###############################################################################
#############
###############################################################################
#############
# Define a service to "ping" the local machine
efine service{
use local-service ; Name of service template to use
host_namelocalhost
service_description PING
check_command
}                                                    check_ping!100.0,20%!500.0,60%

# Define a service to check the disk space of the root partition
# on the local machine. Warning if < 20% free, critical if
# < 10% free space on partition.
define service{
uselocal-service ; Name of service template to use
host_namelocalhost
service_descriptionRoot Partition
check_commandcheck_local_disk!20%!10%!/
}
# Define a service to check the number of currently logged in
# users on the local machine. Warning if > 20 users, critical
```

```
# if> 50 users.
define service{
uselocal-service; Name of service template to use
host_namelocalhost
service_descriptionCurrent Users
check_commandcheck_local_users!20!50
}
# Define a service to check the number of currently running procs
# on the local machine. Warning if > 250 processes, critical if
# > 400 users.
define service{
uselocal-service ; Name of service template to use
host_namelocalhost
service_descriptionTotal Processes
check_commandcheck_local_procs!250!400!RSZDT
}
# Define a service to check the load on the local machine.
define service{
uselocal-service ; Name of service template to use
host_namelocalhost
service_descriptionCurrent Load
check_commandcheck_local_load!5.0,4.0,3.0!10.0,6.0,4.0
}
# Define a service to check the swap usage the local machine.
```

Critical if less than 10% of swap is free, warning if less than 20% is free

define service{

use local-service ; Name of service template to use

host_namelocalhost

service_descriptionSwap Usage

check_commandcheck_local_swap!20!10

}

Define a service to check SSH on the local machine.

Disable notifications for this service by default, as not all users may have SSH enabled.

define service{

uselocal-service ; Name of service template to use

host_namelocalhost

service_description SSH

check_commandcheck_ssh

notifications_enabled0

}

Define a service to check HTTP on the local machine.

Disable notifications for this service by default, as not all users may have HTTP enabled.

define service{

use local-service ; Name of service template to use

host_namelocalhost

service_description HTTP

check_commandcheck_http

notifications_enabled 0

}

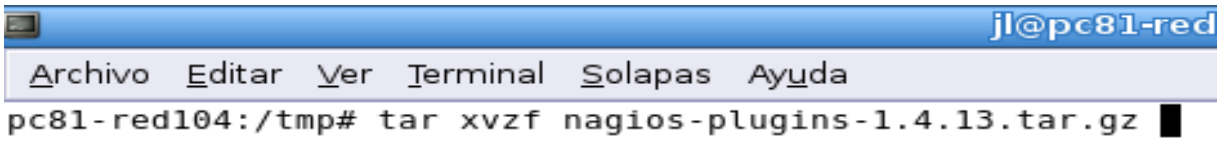
17 Ahora instalamos el archivo de configuración web de Nagios con **makeinstall-webconf** que es ubicado en **/etc/apache2/conf.d/nagios.conf** como se observa en la correspondiente imagen:

```
pc81-red104:/tmp/nagios-3.0.6# make install-webconf
/usr/bin/install -c -m 644 sample-config/httpd.conf /etc/apache2/conf.d/nagios.conf

*** Nagios/Apache conf file installed ***
```

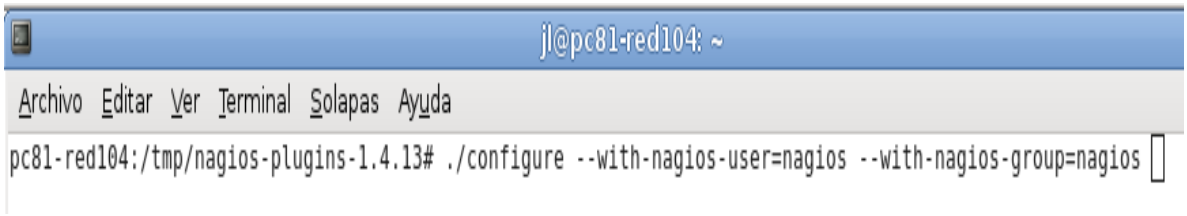
Hasta este ya tendrán instalado NAGIOS en su servidor. Ahora hay que proceder a instalar los **nagios-plugins versión 1.4.13.**

Siempre ubicado en la carpeta /tmp y con utilizando wget tecleamos en la consola de **wget-** http://hivelocity.dl.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-1.4.1 3.tar.gz como en la siguiente se ilustra en la siguiente imagen:

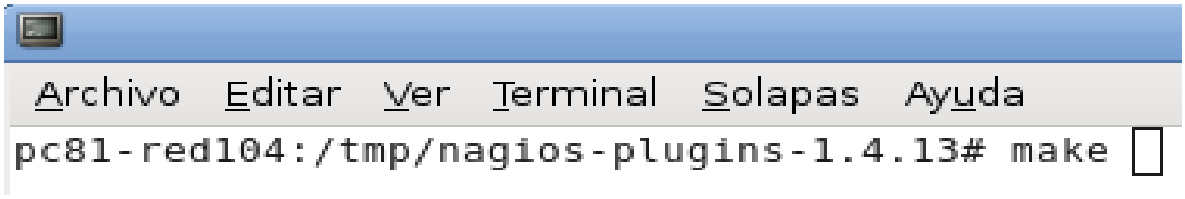
18. Descargados los plugins para Nagios, ahora hay que proceder descomprimirlos con **tarxvzf nagios-plugins-1.4.13.tar.gz** como se ve en la imagen a continuación.



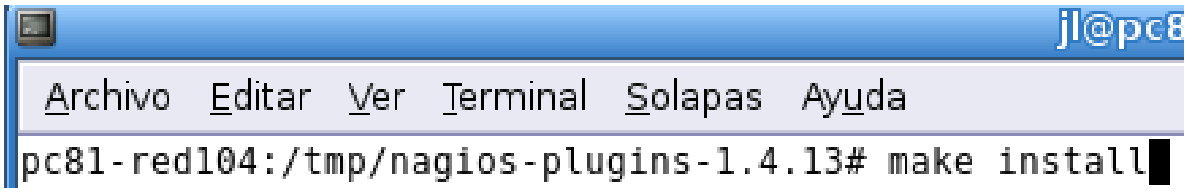
19. Una vez descomprimidos los nagios-plugins hay que ubicarse en la carpeta resultante de la descompresión y correr el scrip de configuración con opciones de configuración para el usuario Nagios y el grupo Nagios como se ilustra en la imagen siguiente.



20. Ahora se procede a compilar los fuentes de los nagios-plugins con **make** como se ilustra en las siguiente imagen:



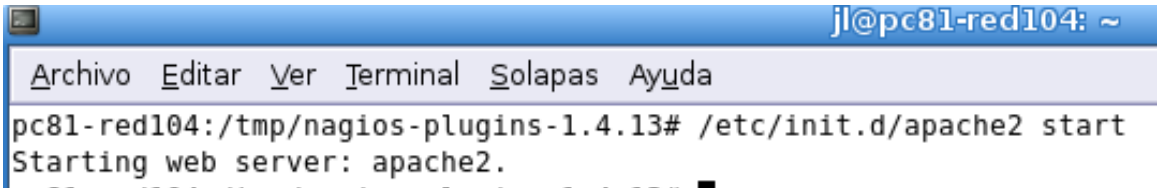
21. Luego se procede a instalar las fuentes compilados con **makeinstall** como se muestra en la imagen:



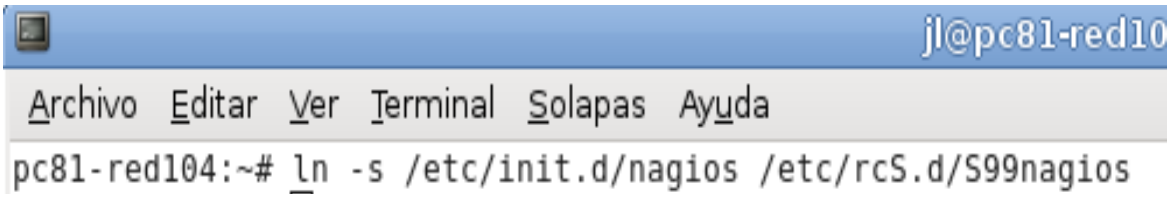
Hasta este momento ya estarán instalado Nagios-3.0.6 y Nagios-Plugins-1.4.13 en nuestro sistema.

22. Lo siguiente que hacer es agregar la contraseña para el usuario administrador de Nagios que es nada más y nada menos que **Nagiosadmin** de esta forma: **htpasswd -c /usr/local/nagios/etc/htpasswd.usersnagiosadmin**

23. Una vez hecho lo anterior procederemos a reiniciar el servidor **Apache** para que se actualice el cambio que se realizo de la siguiente manera:**/etc/init.d/apache2 reload.**

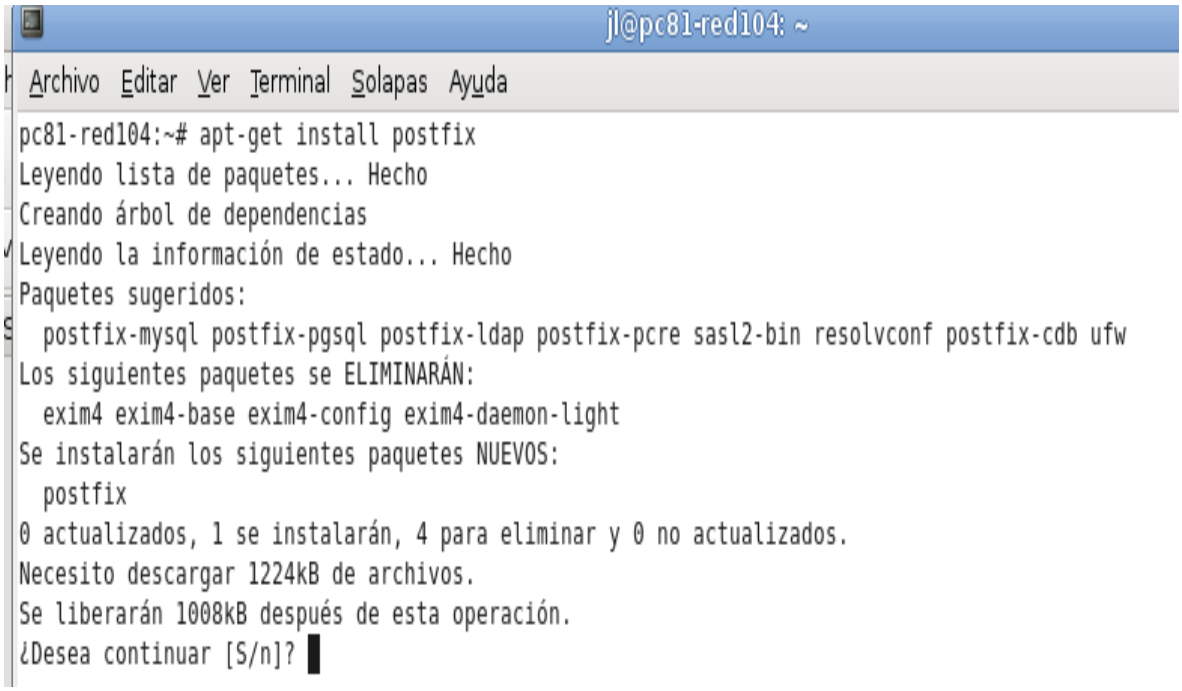


24. A continuación creamos el scrip de inicio de Nagios, para que cada vez que se apague el equipo y se vuelva a encender Nagios se inicie al cargar el sistema operativo donde esté instalado.

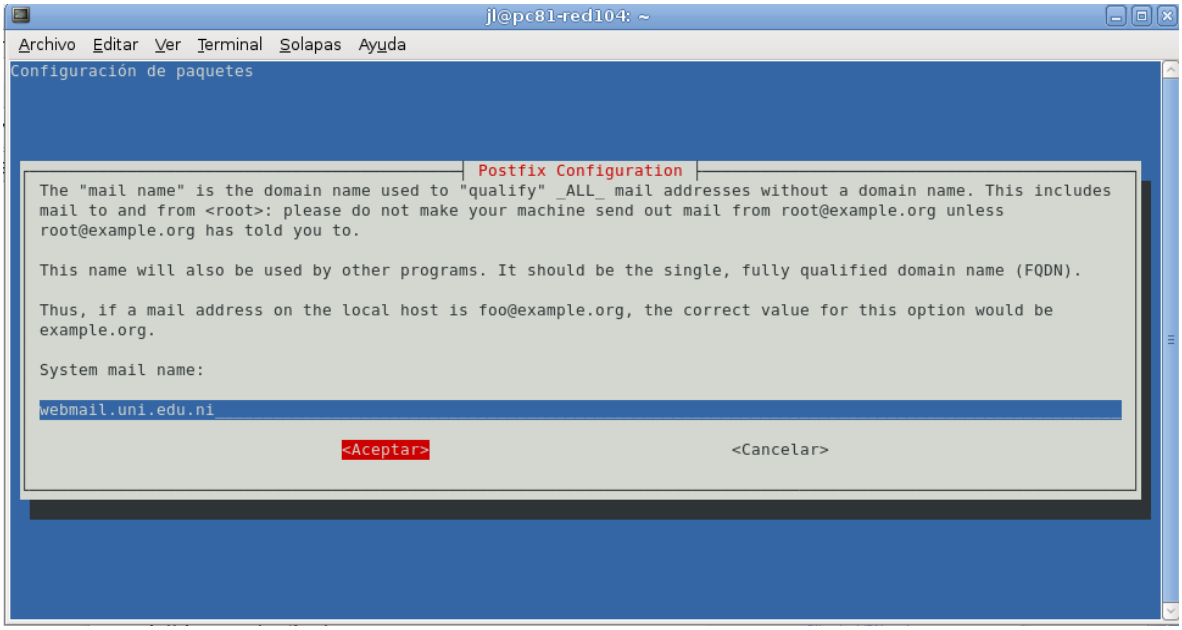


25. Ahora para verificar que Nagios este correctamente instalado abrimos nuestro explorador web y tecleamos la siguiente dirección: **http://localhost/nagios/.**

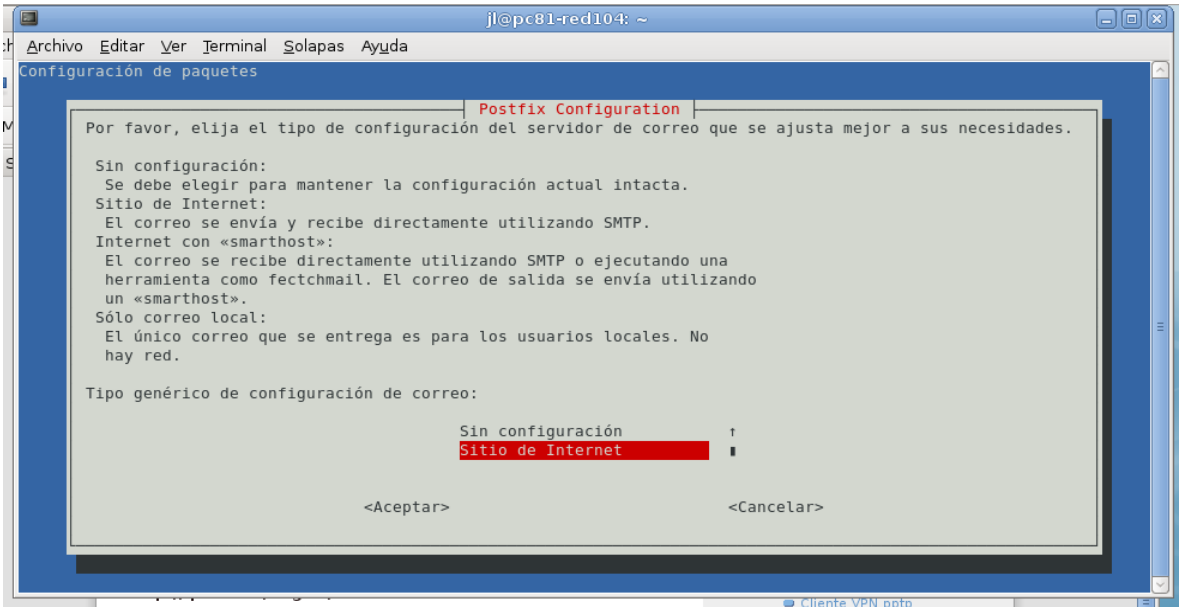
26. Instalar el cliente de correos **postfix** para el envió de alertas a los correos:



27. Luego de eso pasaremos a la configuración de postfix hay que seleccionar sitio de internet: ya que el servidor de corro no está instalado en el Nagios-Server.



28. Luego postfix nos pedirá que en es nuestro servidor de correo saliente o SNMT le damos: http://webmail.minsa.gob.ni



Anexo # 7

Instalación de OCS Inventory

1. Servidor de Base de datos

sudo apt-getinstallmysql-servermysql-client

Durante la instalación ordenaráescribir el password del usuario root de mysql.

2. ServidorWeb

   Instalar el servidorweb apache2

   # sudoapt-getinstall apache2

3. InstalarOCSInventory

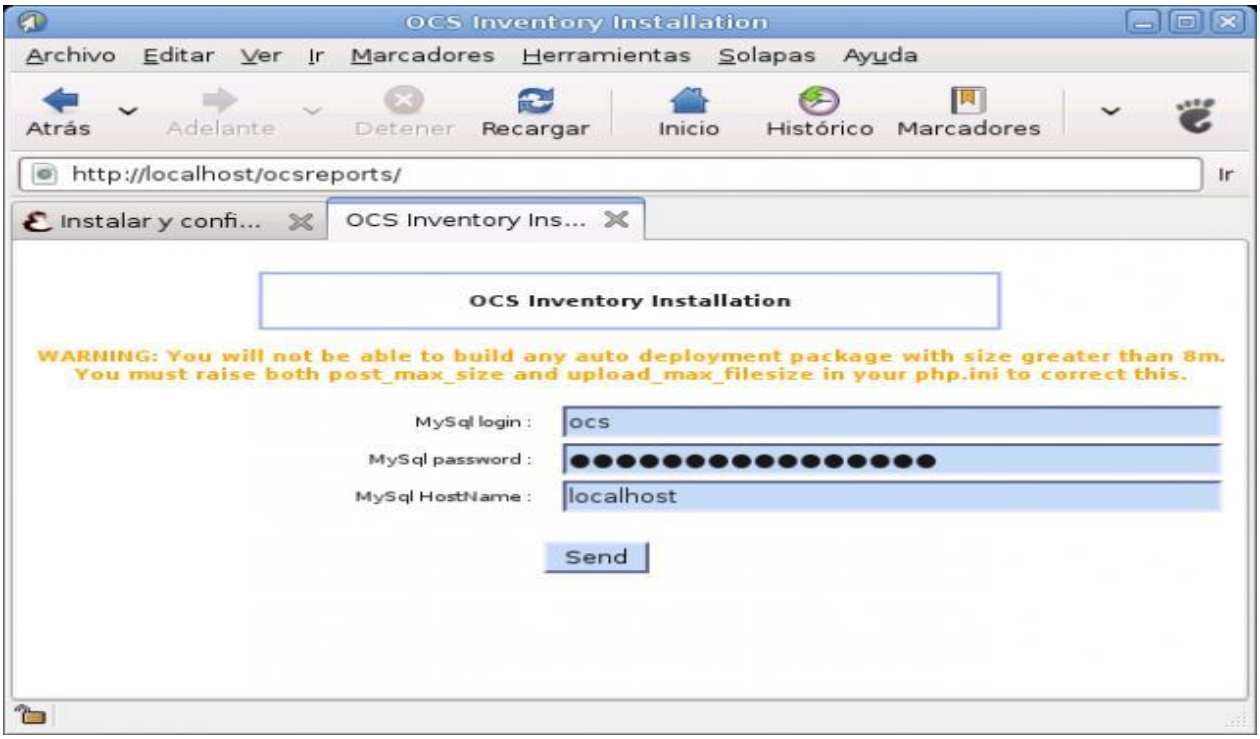
   # sudoapt-getinstallocsinventory-serverocsinventory-reports

4. Para crear el usuario y el password en la consolase ejecuta:

   # sudo htpasswd -c /etc/ocsinventory/htpasswd.setupadmin

5. Se digita el password deseado agregando al navegador web donde se digitará el usuario y password.

6. Solicitará el usuario de la base de datos de ocs-inventory la cual es el root y la clave será la que fue digitada en el paso anterior.



7. Luego aparece un informe sobre la instalación, donde se hará clic ensubmitquery y en el enlace que dice OCS- InventoryNG.

8. Seleccionamos el idioma en las banderas digitando el usuario la contraseña y damos aceptar, el usuario y contraseñas se conservaran desde el comienzo de la instalación.

9. Pasos de la instalación de OCS-Inventory en un cliente Windows

Al realizar el inventario del hardware y software de cada cliente (Pc), es necesario instalar el agente en cada una de las máquinas conectadas a nuestra red, ésta compila toda la información del sistema en un archivo (XML), que será enviado al servidor donde se encuentra el OCS-INVENTORYSERVER, configurado previamente.

10. Pasos previos a la instalación

Antes de iniciar la instalación de OCS-INVENTORY, se recomienda revisar cuidadosamente los siguientes aspectos:

1. Realizar un pingal servidor donde se encuentra el OCS-INVENTORY-SERVER, con el siguiente comando: Ping, dirección IP del servidor ocs-Inventory. Así verificamos la conexión entre el cliente y el servidor.

2. Descargar el agente.

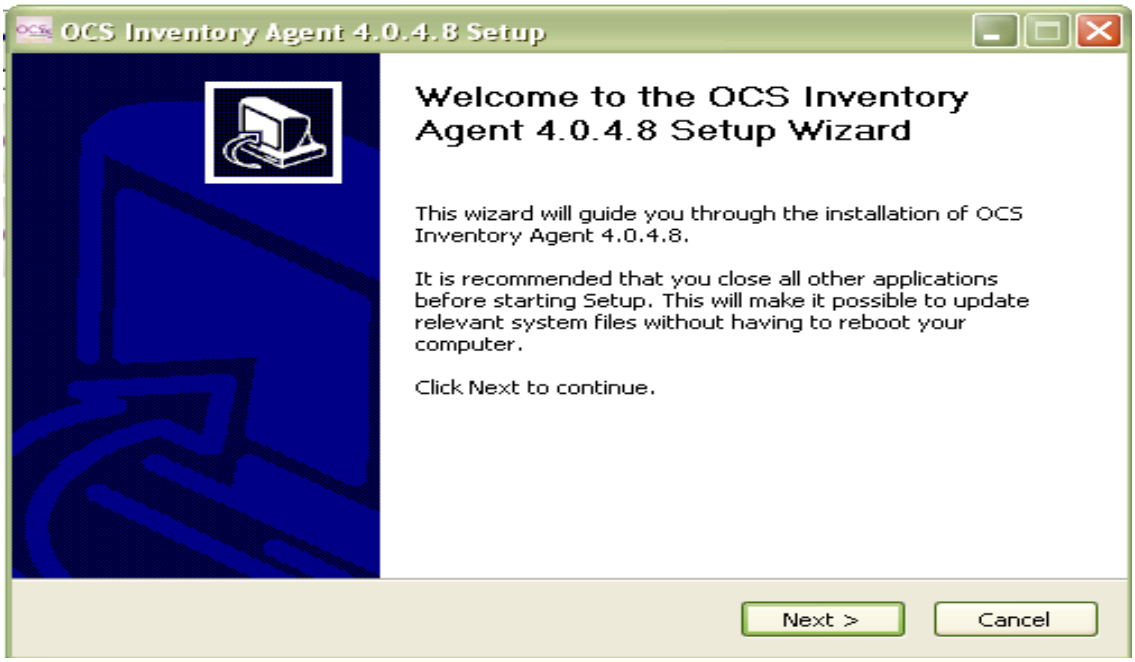
La página web oficial del OCS-INVENTORY. En este caso como se instalo en el servidor de Linux con la versión 1.02_RC2, se descarga la misma versión del servidor digitando la dirección:

http://sourceforge.net/project/downloading.php

Luego se descomprime el archivo y se ejecuta el OcsAgentSetup.exe, se da clip dos (2) veces, para la instalación del agente.

Bienvenido a la instalación del OCS-INVENTORY-AGENTE.

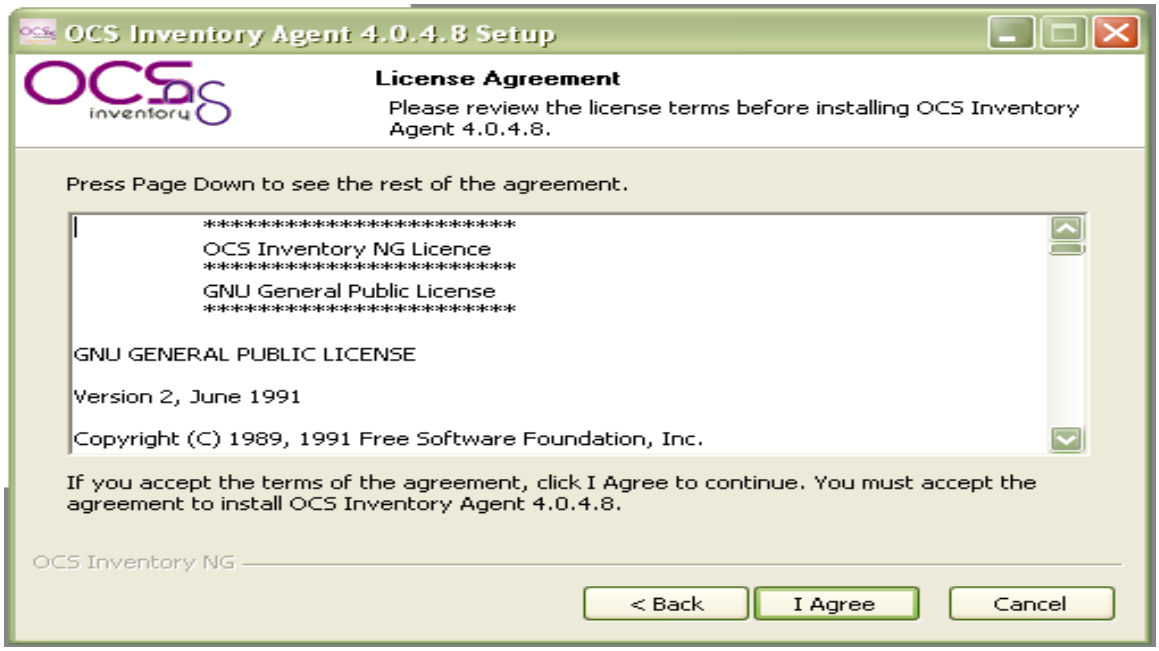
En la pantalla aparecerá presionando la opción siguiente (Next) si deseamos cancelar seleccionamos la opción (Cancel).



2. Acuerdo de Licencia.

En esta pantalla aparecerá la licencia del ocs-Inventory y tendremos tres opciones:

- Back: regresar a la pantalla de bienvenida.
- I Agree: para agregar o aceptar el acuerdo de la licencia.
- Cancel: Cancelar toda la instalación del agente.
- Hacemos clip I Agree para agregar la licencia y continuar con la instalación



3. Configuración del OCS-INVENTORY Agente.

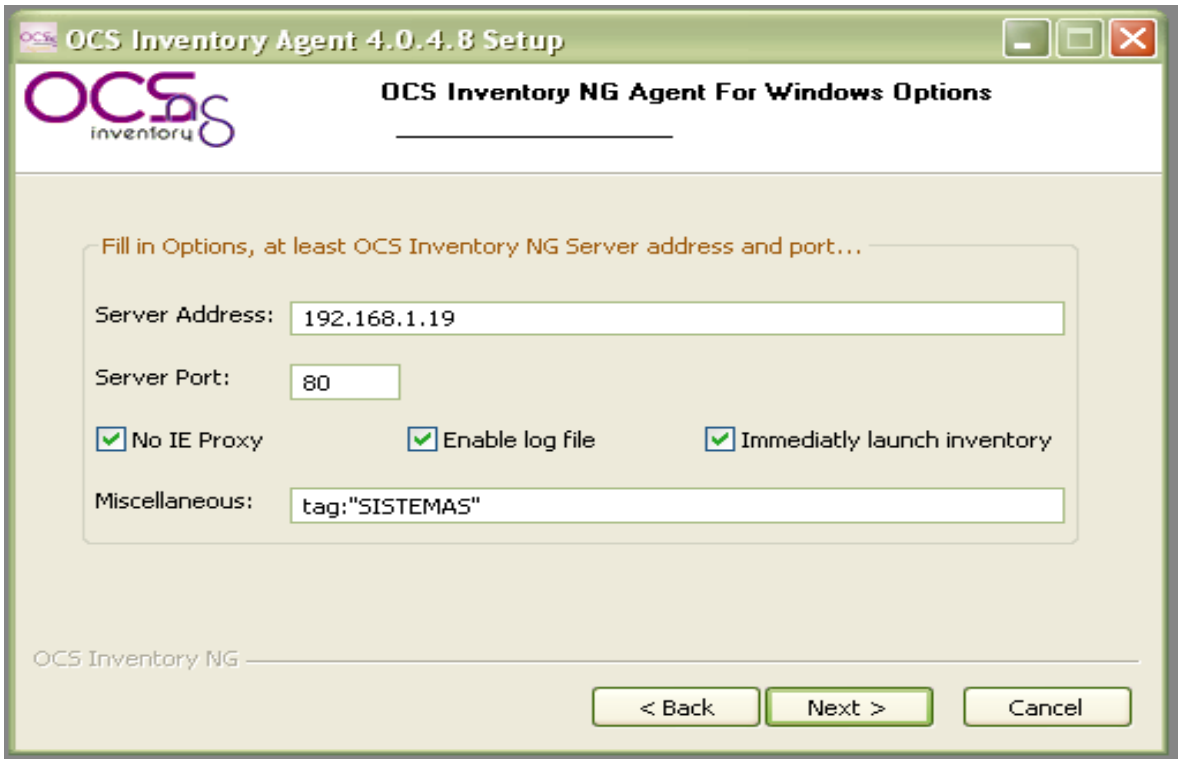
En el Server Address: Se coloca la Dirección IP del servidor del OCS-INVENTORY SERVER.

Server Port: Puerto del servidor por defecto dejamos 80 en server port. Seleccionamos las siguientes opciones:

- No IE Proxy
- Enable log file
- Immediatly launch inventory

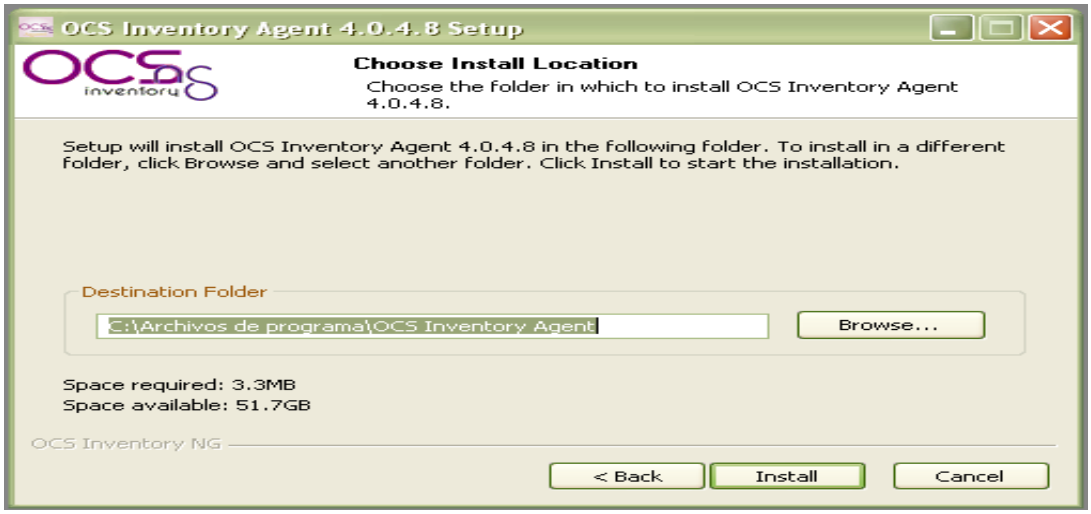
4. Miscellaneous

En este campo se colocan las etiquetas con que se identificará el PC, en este caso, será al departamento donde pertenece el equipo. Para realizar esta operación es necesario instalar esta sentencia /TAG:"NOMBRE DEL DEPARTAMENTO" entonces hacemos clip en (Next) y damos siguiente.



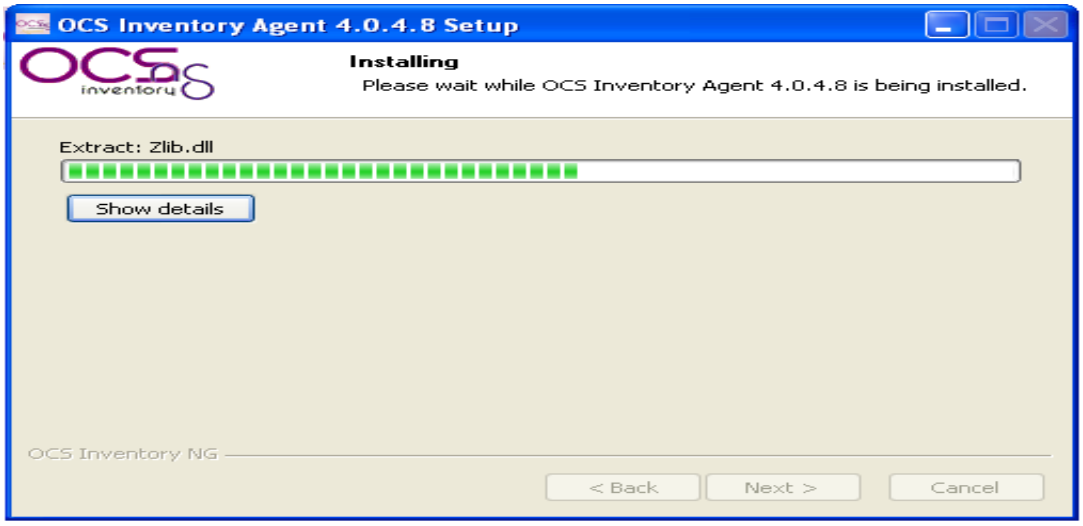
5. Elegir la localización de la instalación.

En el campo de la carpeta destino se conserva la ruta por defecto y presiona rinstall, y se inicia el proceso la ordenación.



6. Proceso de instalación.

Esta sección puede tardar algunos minutos ya que se compila toda la información del equipo además se crea el archivo XML, el cual será enviado al servidor del OCS-Inventory.



7. Finaliza la instalación del Agente

Luego hacemos clip en Finish se culmina la instalación del agente OCS-Inventory.